CPS4EU

Cyber Physical Systems for Europe

D9.2 - Use cases definition and specifications v2

Approver (name – company): Philippe. GOUGEON (VALEO) / Antoine DUPRET (CEA)

Date of approval: 2020/01/26

Dissemination level: Public

Version	Date	Author (name – company)	Comments
V0.1	27/10/2020	G. Giraud (RTE)	**UC10** Upgrade of high level description to show multi-areas, resilience issues, optimization problem Separate Security and Safety requirements Improved high level description of UC10 Feedback from CEA MRE tool and use of dedicated grammar for enhanced functional requirements Simplified visualization of dependencies with PIARCH and components
V0.2	11/12/2020	G. Giraud (RTE Papoz – (SEF)	**UC11** Translation of excerpt from ref [10] in UC11 Analysis of synchro-check and auto-reclosure functions Merge of UC10 and UC11 – For review
V0.3	16/12/20	G. Giraud (RTE)	Reviewed by Antoine RETAGGI (ARCURE) - Ferenc ENDER (SPINSPLIT) Explanation of background for UC11 + minor typos
V1.0	26/01/21	G. Giraud (RTE)	Final version reviewed by TMP

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Table of content

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

0. INTRODUCTION

0.1 Purpose

This document intends to provide a general description of WP9 Use Cases 10 and 11 to WP1-WP6 leaders/participants, so they can better understand the use cases main purposes and the environment where they will be implemented.

0.2 Scope

The following document describes Use cases 10 and 11 of the WP9. A separate document is dedicated to WP9 SME use cases.

These use cases are of special interest to electric grid control. Today's architecture has basically two levels:

- substation control, which performs fast, simple controls based on local information (such as voltage and currents in the substation),
- control room, which includes wide area, slower controls, (such as load frequency control or global secondary voltage control).

With the rise of distributed generation, a different control architecture may be needed. If a consensus seems to emerge in the academic community on the use of distributed control to manage complex systems (or systems of systems), the electricity industry is still working on what should be this future control architecture.

RTE R&D is promoting a 3-layer architecture, where "area" controls are supplementing the 2 existing layers.

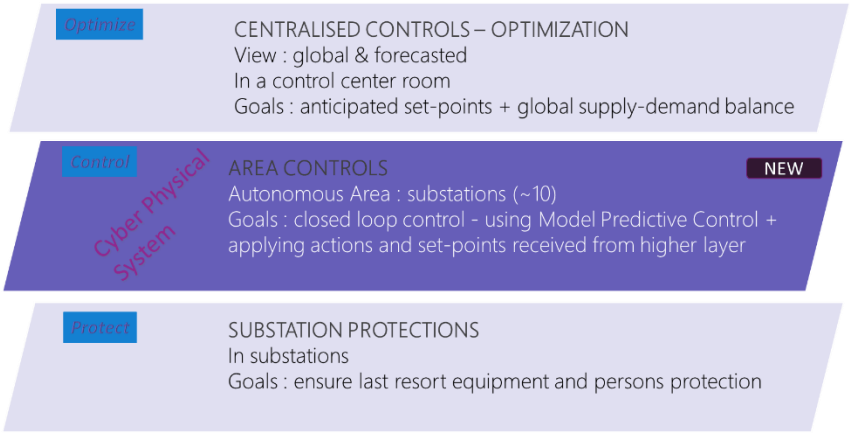


Figure 1 - Three layers model

The centralized level handles the global vision and the heavy forecasting computation and provides lower levels with set points for optimal operation (OPTIMIZE).

The area level applies actions from higher level and reacts to any unforeseen problems to adapt in real-time (seconds) the strategy (CONTROL).

Substation protection take immediate actions (milliseconds) to guarantee people and assets protection, such as opening breakers when short-circuit is detected (PROTECT).

The use case 10 is the first implementation of this "area" concept on RTE transmission grid. The use case 11 is the application of virtualization technologies to the Protect layer with significant real-time constraints.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

0.3 Link to other documents/TASKS

ID	Description
D4.1	Specifications of collaborative mechanisms
D4.3	Specifications of prototypes of the framework
D9.1	Use case requirements v1

0.4 Definitions, acronyms, and abbreviations

Acronym / abbreviation	Description
µP	Microprocessor
AC	Alternative current
ADC	Analogue to digital converter
API	Application Programming Interface
BoM	Bill of Materials
CB	Circuit Breaker
CPTS	Compute server
CPT	Compute
CSS	Control & Storage Server
CT	Current Transformer
CTL	Control
DER	Distributed Energy Resources
DSO	Distribution System Operator
FMEA	Failure Modes & Effects Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
GB	Ground Benign environment
HW	Hardware
ICCP	Inter Control Centres Protocol
IED	Intelligent Electronic Device = digital protection relay
MPC	Model Predictive Control
(SA)MU	Merging Unit
MUX	Multiplexer
NAZA	New Area Zonal Automatons
POC	Proof Of Concept
PP1	Principal Protection 1
RAM	Reliability Availability Maintainability
RBD	Reliability Blocks Diagram

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Acronym / abbreviation	Description
SDEC	Software Defined Edge Control
STB DI	Smart Terminal Block Digital Input
STB DO	Smart Terminal Block Digital Output
SW	Software
UE	Undesirable Event
TSO	Transmission System Operator
VT	Voltage Transformer

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

1. REQUIREMENTS GATHERING METHODOLOGY

This section reports the methodology adopted in tasks 9.1/9.2 to define the requirements related to the CPS4EU Energy use cases. In the following paragraphs the type of requirements, the adopted notation and the requirement code conventions are described.

Requirements play major roles as they:

- Form the basis of system architecture and design activities
- Form the basis of system integration and verification activities
- Act as reference for validation and stakeholder acceptance
- Provide a means of communication between the various technical staff that interact throughout the project.

1.1 Requirements Types

According to the IEEE Standard Glossary of Software Engineering Terminology[1], a requirement is:

- A condition or capability needed by a user to solve a problem or achieve an objective
- A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents
- A documented representation of a condition or capability as in (1) or (2).

CPS4EU Energy and SME (WP9) Use Case requirements are classified into the following types:

Functional Requirement	A requirement that specifies a function that a system, or system component, must be able to perform. A requirement specifying **what** the overall system, or a specific component, will be able to do. Statements of services that the system should provide, how the system should react to particular inputs and how the system should behave in particular situations. Among the functional requirements are also included security requirements relating to the security services offered by the system to users or other systems.
Non Functional Requirement	A requirement specifying **how** the system or component will implement its functionality. In this document the following non-functional types of requirements are considered: • Interface Requirements • Performance Requirements • Security Requirements • Safety Requirements • Operational Requirements • Usability Requirements • Policies & Compliance Requirements • Design Constraints • Ethical Requirements • Other Requirements.

The following table describe each requirement type:

[1] https://ieeexplore.ieee.org/document/159342/definitions#definitions

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Requirement Type	Req.ID	Requirement Description
Functional Requirement	**FNC**	Functional Requirements describe the behaviour and information that the solution will manage. In the case of a non-system solution, the behaviour typically refers to a workflow and the information refers to the inputs and outputs of the workflow. Additionally, the requirements describe how the data will be transformed and by whom. In the case of a system solution, the functional requirements describe the features and functionality of the system as well as the information that will be created, edited, updated, and deleted by the system.
Interface Requirement	**INT**	Interface requirements define how the system is required to interact or to exchange information with external systems (external interface), or how system elements within the system interact with each other (internal interface). Interface requirements include physical connections (physical interfaces) with external systems or internal system elements supporting interactions or exchanges. External interface requirements are important for embedded systems and outline how your product will interface with other components. There are several types of interfaces you may have requirements for, including: • Hardware: Describe the logical and physical characteristics of each interface between the software product and the hardware components of the system. • Software: Describe the connections between this product and other specific software components (name and version), including databases, operating systems, tools, libraries, and integrated commercial components. Identify data that will be shared across software components. • Communications: Describe the requirements associated with any communications functions required by this product, including e-mail, web browser, network server communications protocols, electronic forms, and so on. Identify any communication standards that will be used, such as FTP or HTTP. Specify any communication security or encryption issues, data transfer rates, and synchronization mechanisms.
Performance Requirement	**PRF**	If there are performance requirements for the Use Cases under various circumstances, state them here and explain their rationale, to help the developers understand the intent and make suitable design choices. Specify the timing relationships for real time systems. Performance requirements can refer to individual functional requirements or features (e.g. speed of response for a certain functionality).
Security Requirement	**SEC**	Security requirements are related to both the facility that houses the system(s) and the operational security requirements of the system itself. Specify the security and privacy requirements, including access limitations to the system, such as log-on procedures and passwords, and of data

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

		protection and recovery methods. This could include the factors that would protect the system from accidental or malicious access, use, modification, destruction, or disclosure. Examples: • Access requirements • Integrity requirements • Privacy requirements.
Safety Requirement	**SAF**	Safety requirements are derived from safety goals and safety policies (as well as from hazard analyses) and aim at risk reduction. In safety-critical embedded systems, this might incorporate a distributed log or history of data sets, the assignment of certain functions to different single systems, or the restriction of communications between some areas of the system.
Operational Requirement	**OPR**	Examples: • Delivery mode • Access mode • Availability • Maintainability • Reliability • Capacity • Scalability • Portability • Installation.
Usability Requirement	**USB**	Examples: • Environment of use • Appearance and style • Ease of use • Internationalization • Accessibility.
Policies & Compliance Requirement	**P&C**	These requirements identify relevant and applicable organizational policies or regulatory requirements that could affect the operation or performance of the system(s). Examples: Laws and regulations, standards, business rules.
Design Constraint	**DSG**	Example: Environmental Requirements, which identify the environmental conditions to be encountered by the system in its different operational modes. This should address the natural environment (e.g. wind, rain, temperature, fauna, salt, dust, radiation, etc.), induced and/or self-induced environmental effects (e.g. motion, shock, noise, electromagnetism, thermal, etc.), and threats to societal environment (e.g. legal, political, economic, social, business, etc.).
Ethical Requirement	**P&E**	See §5.1 Ethics of CPS4EU proposal, with particular reference to the document “Ethical Aspects of Cyber-Physical Systems”: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU%282016%29563501_EN.pdf
Other Requirements	**OTR**	Any other requirement that cannot be classified with the above categories.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

1.2 Requirement Identification

The CPS4EU Use Case requirements will be uniquely identified by an alphanumeric code consisting of:

<*Use Case number*>-<*classification*>-<*number*>, where:

<Use Case ID>	**UC10**	Distributed controls for transmission network
<classification>	**FNC**	Functional Requirements
	INT	Interface Requirements
	PRF	Performance Requirements
	SAF	Safety Requirement
	SEC	Security Requirements
	OPR	Operational Requirements
	USB	Usability Requirements
	P&C	Policies & Compliance Requirements
	DSG	Design Constraints
	ETH	Ethical Requirements
	OTR	Other Requirements
<number>	A progressive number that uniquely identifies the requirement within a requirement type.	

Example:

UC1-USB-01 → Use Case: UC1, Requirement type: Usability Requirement, Requirement number: 01

1.3 Requirement Principles

The following principles apply:

Characteristics	Specific requirements should comply with the following characteristics: • unambiguous • complete • consistent • ranked for importance and/or stability • verifiable • modifiable • traceable
Cross-references	Specific requirements should be cross-referenced to earlier documents that they relate to.
Readability	Careful attention should be given to organizing the requirements to maximize readability.
IDs	All requirements should be uniquely identifiable (via ID).

Each requirement should also be **testable**, i.e. from which test cases could be designed which would demonstrate clearly, unambiguously, and cost-effectively whether the requirement is met.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

1.4 Requirement Attributes

Each requirement will be classified according to the following ***Priority***:

Priority	*Feature*	*How to describe it*
High	A required, must have feature	The system **shall**…
Medium	A desired feature, but may be deferred till later	The system **should**…
Low	An optional, nice-to-have feature that may never make it to implementation	The system **may**…

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2. UC10 - DISTRIBUTED CONTROLS FOR TRANSMISSION NETWORK

2.1 Overall Description

2.1.1 High level Use Case Description

Renewable Energies, and especially Distributed Energy Resources (DER), are increasingly important in electricity generation, especially wind and solar power, and pivotal for the energetic transition. From a system operation point of view, they differ in many points from classical power stations:

- They are often **connected to lower voltage networks**, not designed to accommodate generation.
- They have very **variable outputs**, depending on meteorological factors (for example, wind farms produce on average 25% of their peak power).
- Their average unitary power is lower than classic power stations, so system operators will interact with significantly **higher number of actors**.

An electrical network is dimensioned to manage the **peak current**, so DER could lead transmission operators to build power lines used only a fraction of the time. A more optimal alternative is to manage the flow using new possibilities offered by batteries, power electronics and cyber-physical systems to operate the grid closer to its limits: less physical, more cyber.

For example, on the network presented on Figure 2 , green arrows represent a current under the acceptable limit whereas the red arrow represents an overload on the line between A and B. Transmission network (TSO) is in orange, distribution network (DSO) in purple.

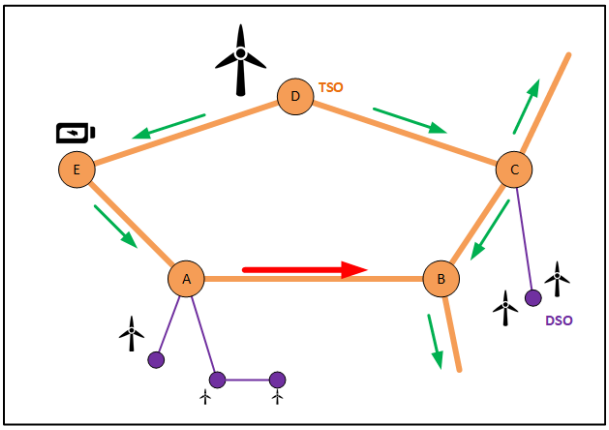


Figure 2 - Load constraint

Different levers can be activated to remove this constraint:

- Charging the battery in E,
- Limiting production in D,
- Limiting production at DSO level in grid connected to substation A.

Most of the time, it is a combination of these actions that will be the most relevant, given several parameters: state of battery's charge, time to limit production of the wind farms, severity of the overload, values of currents on the other lines, state of the network after the use of these levers, generation merit order (curtail the cheapest wind farm first), …

The time-to-action is too fast for a human operator (dozens of seconds max) and the complexity of the optimization is beyond its grasp. That is the reason why we need to install distributed controls, called New Area Zonal Automaton systems (NAZA), to handle this task.

By monitoring the network and simulating the flows, **the NAZA system** will ensure the safe operation of the network (in nominal or n-1 situations) by sending:

- topological orders to the network **circuit breakers**,
- **modulation** orders to the **generators**,
- set points to the storage **batteries**.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

The distributed nature of these controls can be considered at two levels:

- A distributed algorithm, with one algorithm per area,
- A distributed infrastructure, which supports these algorithms.

When NAZA has by nature a distributed algorithm, the infrastructure can be centralized (in a datacenter), distributed (in the substations) or hybrid (datacenter + substations). RTE will use a centralized architecture to validate the algorithm, but will then experiment a distributed infrastructure as described in this use case in Figure 3 - NAZA physical implementation.

The NAZA system is composed of interfaces called **NAZA acquisition** to monitor and act on the network, of calculators called **NAZA cores** who implement the optimisation algorithms, of **telecom links** to ensure communication between its distributed components (Figure 3). They act on the **levers**: wind and solar farms, batteries, network topology …

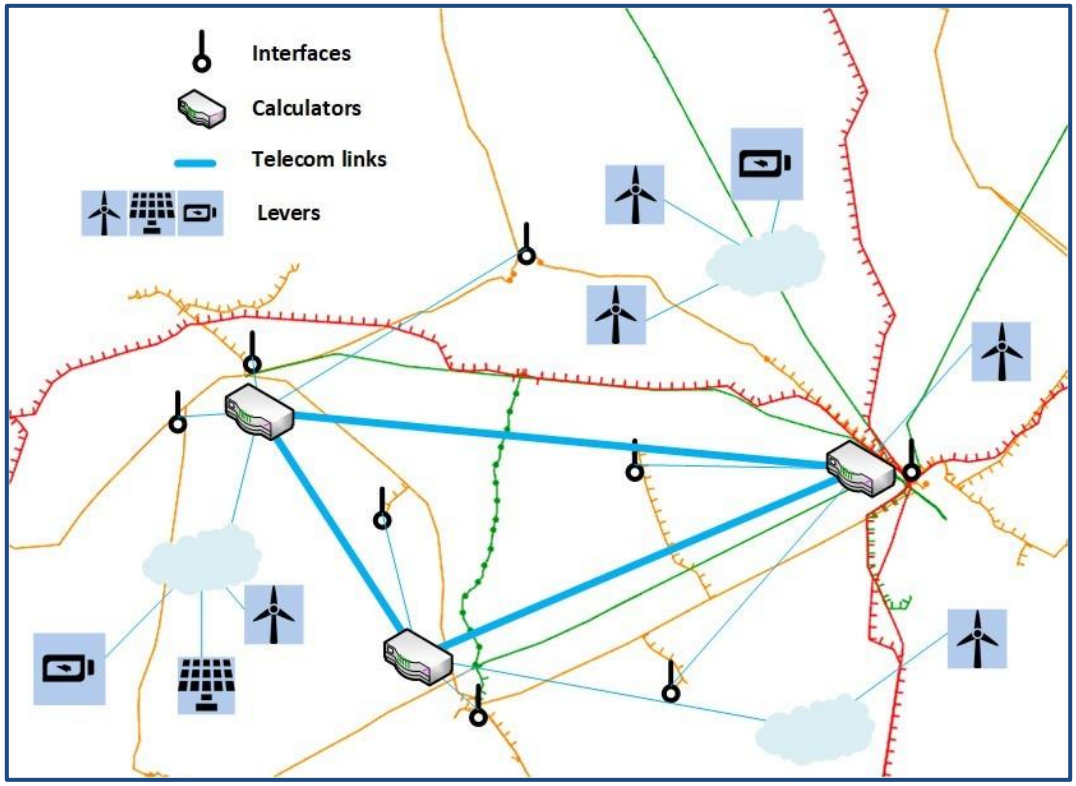


Figure 3 - NAZA physical implementation

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

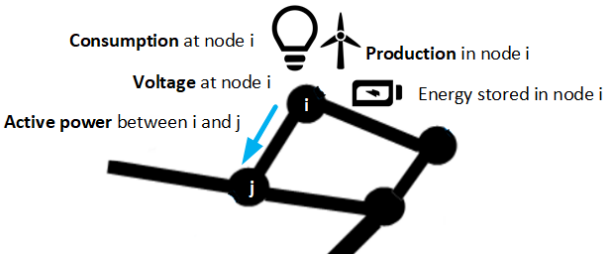
As load constraints can appear in very diverse network situations, the use of predefined solutions is not a valid method. Rather, we formed a real-time **optimization model**[2] (Figure 4) and solve it on the area. It includes:

- The network equations[3] (active only),
- Modelling of levers (in particular the time to action),
- The equations for the evolution of the energy stock in the battery as a function of the charged/discharged power.

Physical **constraints** (transit limits on the lines, batteries levels, total generation to be curtailed) are associated to the model.

The **state of the system** is represented at any time by:

- The voltage phases in each node i,
- The active power on each line (i,j),
- The energy stored in the battery i,
- The production g in each node i,
- The consumption c in each of the nodes i, including flows into or out of the area.



The **cost function** reflects the impact on the grid (deviation from planned transits and batteries set-points) and the cost of the levers (curtailed generation, battery use). For the congestion management of the areas studied in the current NAZA framework, the objective function of the optimization model is the minimization of the generation curtailment.

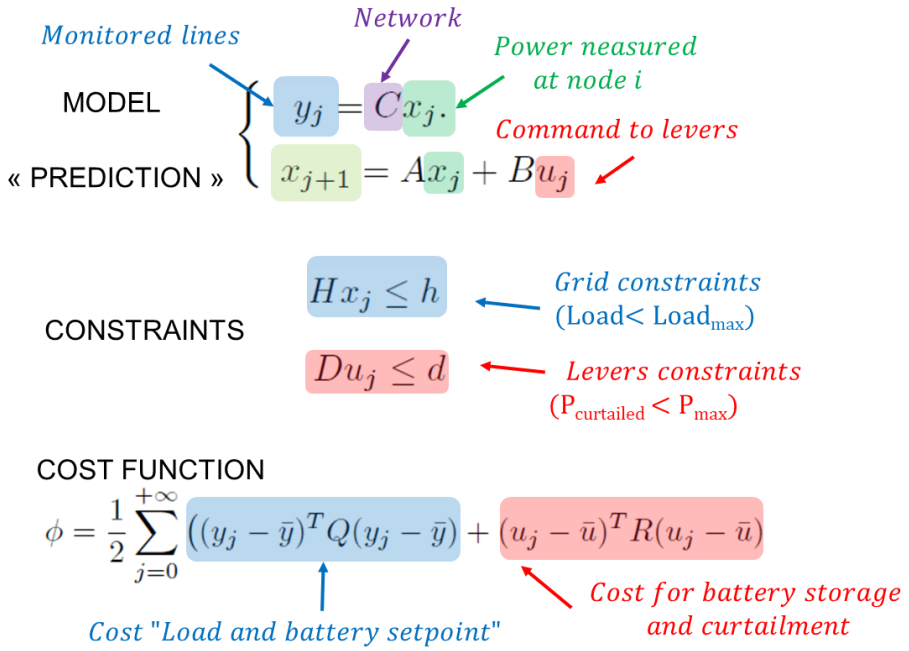


Figure 4 - Model Predictive Control equations

The algorithm takes into account **temporal aspects**, especially for how long has a load threshold been crossed or what are the delays of the actions already sent. This aspect of the problem oriented the

[2] Zonal congestion management mixing large battery storage systems and generation curtailment (Authors: Clementine Straub, Sorin Olaru, Jean Maeght, Patrick Panciatici) arXiv:1806.01538

[3] approximation of direct current, voltage aspects are not modelled

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

choice to Model Predictive Control which uses a time horizon window.

The NAZA system chooses which generation to power off, which generation to limit and at what value, which charge or discharge power to request from the battery according to the network conditions, and more generally which lever to use. Still, the calibration of this model, i.e. the margins associated to each type of levers, has to be determined for every area. The **auto-calibration** of these parameters is to be investigated during the CPS4EU project. Also, the **robustness** of the algorithm to uncertainties in the model (e.g. time to action of wind farms) or in the data (handling of absent or corrupted measurement) has to be assessed.

Information from the **centralized system** (Figure 1 - Three layers model) is sent to the NAZA system, most notably loads and voltages from outside the area, overall network topology, batteries set-points or generator capabilities. Should this information be missing, the NAZA system shall continue to operate, even in downgraded mode, for several minutes, as this information has slow dynamics.

As renewable generation arrive on the grid, projections show that the need for NAZA systems will strongly grow over the years (Figure 5 - NAZA forecasted deployment).

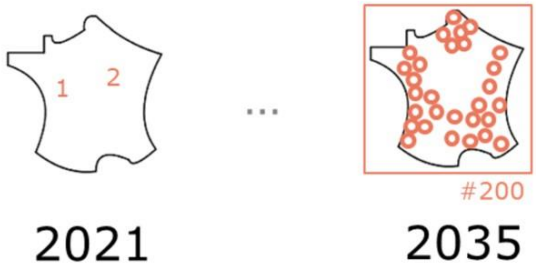


Figure 5 - NAZA forecasted deployment

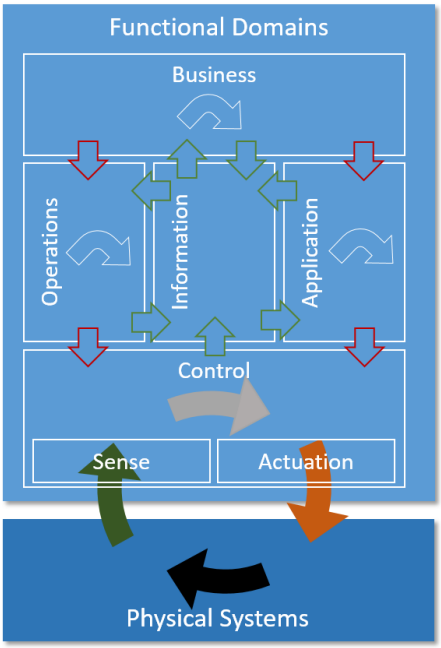
This situation will lead to growing interactions or even overlaps between different NAZA areas. Hence, scalability of the solution is a strong requirement. The problem of the cooperation between several distributed MPC in non-independent areas is also to be addressed.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2.1.2 Main Features

We describe the functional domains using the "Industrial Internet of Things Volume G1: Reference Architecture"[4] nomenclature to describe the NAZA system main features.

Control domain



The system **acquires data** (getters) from the sensors (current and voltage transducers, position relays, weather sensors…) installed in the substations of the area. This function can include aggregation or basic combination of acquired data (e.g. turning high frequency Sample Values into RMS values). Rate of acquisition varies from 10s (actual sensors) to 1s or less.

It **writes data** to actuators (setters): Open/close orders to circuit breakers or isolators, set-points to batteries, generation limit value to generators…

It allows **communication** between all these elements (sensors, actuators, gateways, computation units), located in several distant locations. This layer also provides **entity abstraction** so every element of the system can be accessed in a standard way, whatever protocol it uses (IEC 61850, 60850-6-104, Modbus, OPC-UA, ICCP…).

Modelling gives meaning to the retrieved information. It associates a value with a part of the electrical network, i.e. a sensor value to the voltage of the X bus in the Y substation. It maps the data from sensors or actuators to the network model provided to the system (IIDM - iTesla Internal Data Model from the POWSYBL project[5]).

Asset management function includes:

- on boarding (if possible auto discovery) of new components (nodes, gateways),
- basic surveillance of components (NOK/OK), updates of configuration, policy, system or software/firmware updates,
- dynamic resources allocation (for availability or performance issues).

Executor implements the control logic given the states, conditions and behaviour of the system under control and its environment. It relies on the **Model Predictive Control** with a solver that optimize a cost function to use levers such as batteries set-points, generation limit values, … Simple flow charts enforce safety rules in case no solution is found or computation takes too long. For example, they may result in curtailing all necessary generation.

Operations domain

These functions are common to all, or at least several areas that implement NAZA systems.

Provisioning and deployment allows to on-board, configure and register assets from a central operation room at scale, for example upgrading all devices from an area at the same time.

Modification of control logic in executor, for example by implementing a new code for optimization, is part of **managements** function.

[4] https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[5] Powsybl (Power system blocks) is an open source framework written in Java that makes it easy to write complex software for power systems' simulations and analysis. Its modular approach allows developers to extend or customize its features. Powsybl is part of the LF Energy Foundation, a project of The Linux Foundation that supports open source innovation projects within the energy and electricity sectors. Powsybl in an open source framework licensed under the Mozilla Public License 2.0.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Monitoring and diagnostics combine:

- Detection of real-time problems by collecting sensors health data,
- Advanced diagnosis of the root cause of this problem,
- Alert on abnormal conditions.

Optimization is in charge of global optimization of resources devoted to the different NAZA systems, to improve reliability and efficiency.

Information domain

Data from the sensors is sent to the control centre level, possibly after filtering. It may be used by Centralized Slow Automata or other applications. It is also stored in a data lake for subsequent analysis.

Specifically, orders sent to generators and batteries are sent to the back-office for settlement purposes, that should be demonstrated in the OneNet project. State of each NAZA system is also sent to telecontrol system.

All events are available in an execution log for feedback and troubleshooting analysis.

Application domain

Logic and rules are part of the centralized system (Figure 1 - Three layers model). They won't be described here, but an example is the batteries pre-calculated program, which is computed by application domain by centralized system and sent to NAZA systems to be applied by control domain. Weather forecast or any useful data are also transmitted to control domain.

UI shows to control room operator the state of NAZA system, the values measured by sensors and the set-points or limits sent to batteries and generators. Operators can also put in or out of operation a specific NAZA system. Another UI allows specialists to change the logic of the automata and to deploy it by invoking management function from the operations domain.

API with SCADA system and hypervision system will also be considered in the future to provide a seamless integration in the control room. The NAZA dedicated HMI will then only be used as a back-up as all operations in the control room should use the OperatorFabric platform.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2.1.3 Limits

The functions of the NAZA system are distributed between several components (from a hardware and software point of view) so it maximizes its capacity to operate under severe conditions (software or hardware breakdowns, communication failure…).

Maximum reliability is expected for control domain functions that must be able to operate even if other functions are unavailable.

Typical application needs a maximum delay between data acquisition and order around 10s, but shorter operation times will be sought.

Coupling with other applications should be loose, so RESTful implementation is preferred.

Fan-less hardware is favoured for use in the substations, with an extended temperature range of operation.

Linux OS is required and the use of a secured CentOS (7.4) is mandatory.

Java or C++ are currently in use in RTE development teams.

Open Source code is mandatory.

Communication protocols common in the electric utility are used at the interfaces: IEC 60870-5-104, 61850, ICCP. Bandwidth between substations can be limited to 500kb/s, so communication sobriety is a plus.

Due to the criticality of the application, security should meet the highest standards. Whenever decided by cybersecurity team, security patches have to be applied.

2.1.4 Conclusions

This system focus must first of all be security of operation, with means it should not send **unwanted** commands. By adopting a decentralized or distributed architecture, we aim to boost its **dependability**, i.e. its ability to issue valid commands, even in non-nominal conditions.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2.2 Requirements

The **complete use case 10 requirements are detailed in Appendix 4.1**, with a level of detail sufficient to enable CPS4EU designers to design components and pre-integrated architectures to satisfy those requirements, and testers to test that the system satisfies those requirements.

The **main points** are summed up hereafter.

Functional requirements put emphasis on the timing for data acquisition and for the command sent to levers (circuit breakers, batteries and generators). A supervisor component handles the operating mode of the system (normal, fault, trial). The MPC algorithm internal behaviour is not described here and is considered as a black box.

Interfaces handle the conversion of the different data standard from telecontrol sensors to the internal model. Internal exchanges are on https REST exchanges. Interoperability with existing systems is also a concern. Limitation of bandwidth available in substation is taken into account.

Performances are far from “hard” real-time systems but dependability and availability are important parameters. **Design** is adapted to field constraints such as no or poor air-conditioning in substations.

Security and safety requirements are specific to electric networks standards with special concern for safety of persons and goods and use of secure operating system. **Compliance to policies** such as NIS and **ethics** are of course mandatory.

Operation features are important since NAZA systems will be in unmanned substation and should be remotely operated and monitored. The system has to conform to **usability** standard for control rooms systems and has to offer the possibility to be connected to a hypervisor system.

This use case should rely on WP6 **Cooperative PIARCH** (A4) and components from WP4 **cooperative algorithms**.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3. UC11 - SUBSTATION DIGITALIZATION

3.1 Background – Use case

3.1.1 Traditional substation automation

A substation automation system is a collection of hardware and software components that are used to monitor and control an electrical substation, both locally and remotely. A substation automation system also automates some repetitive, tedious and error-prone activities to increase the overall efficiency and productivity of the system.

Even if most functions can be mutualized on the same hardware, protection functions, which are critical for safety as they are in charge of electric fault elimination, are process by dedicated intelligent electronic devices (IED). These IED can collect and record information on many different parameters of a system, process them based on complex logic in a fraction of a second and make decisions on abnormal situations to send control commands to switches and breakers to clear the fault.

In a typical transmission substation (Figure 6 - Typical HV transmission substation), this means at least one protection relay (P44x) per line or transformer feeder, in addition of another IED (C264) for automation functions shared between 2 feeders.

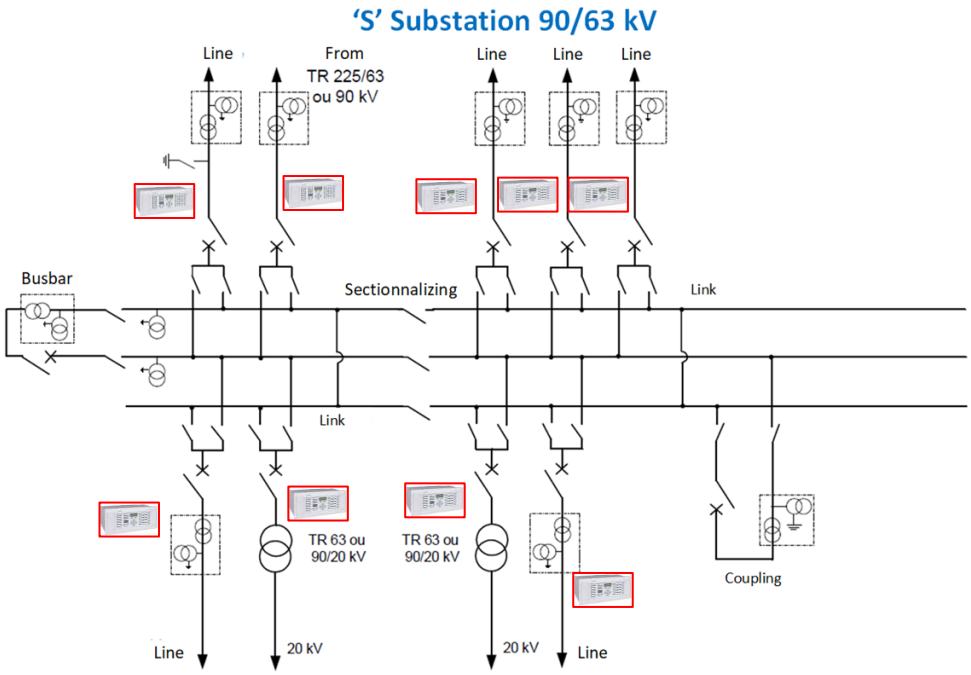


Figure 6 - Typical HV transmission substation

These IED located next to the feeders communicate with central devices located in the substation main building. These central devices are in charge of substation areas automation and communication with the central SCADA through the Remote Transmission Units (RTU).

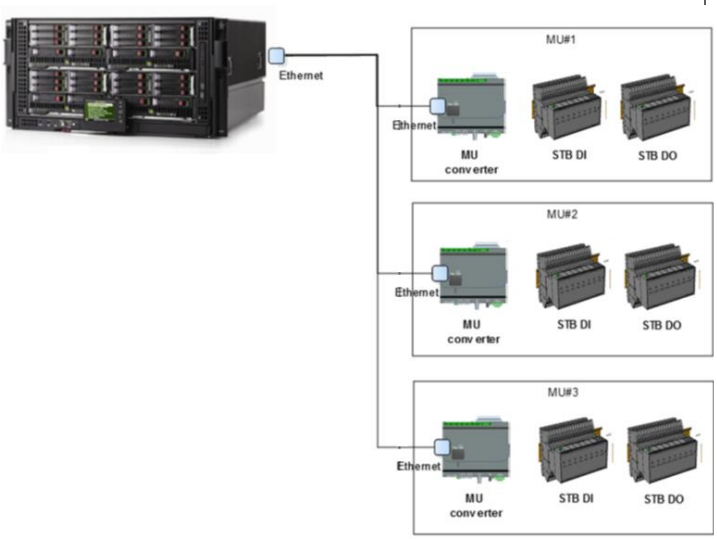
This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.1.2 The innovative Software Defined Edge Control approach

A Proof Of Concept project is currently ongoing at Schneider Electric, based on virtualization technology.

This innovative approach, named **Software Defined Edge Control (SDEC)**, consists in replacing the classical protection relays (i.e. IEDs such as P44x) and automation (i.e. IED such as C264) by a new distributed solution, where all these functions are virtualized on two servers (for redundancy) for the whole substation.

This minimizes the complexity of the field equipment of an electrical substation, and relocate the treatments ("the intelligence") in servers at the Edge level (substation) instead of being spread through the different feeders. Typically, in a 8 feeders substation, the number of equipment could fall from at least 12 IED (8x1 P444 for protection and 4x1 C264 for automation) to 2 servers.

Classical solution based on Micom IEDs and C264 controllers (at least one IED per HV circuit breaker)	**SDEC solution** (reduced field equipment, intelligence at EDGE level)
 **Micom P44x protection relay**  **Micom C264 bay controller**  **Micom P44x protection relay**	

RTE is in partnership with Schneider Electric in the scope of this virtualization project. Both partners want to evaluate the benefits and the limits of this new technology, in particular dependability investigations.

This document recalls the work done on the distance protection ANSI[6] 21 exposed in D9.1 and extends it to two new functions:

- The ANSI 25 "synchro-check" protection
- And the "automatic recloser" ANSI 79 function.

Note: As line feeder is the most common HV structure in substation, the study focuses on common line protection and automation functions, such as distance protection, synchro-check and automatic recloser.

[6] The ANSI (American Institute of Electrical Engineers) has codified electric devices and functions. The complete list can be found in IEEE C37.2-2008 – "IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations" or on Wikipedia.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.2 Purpose of the document

This document summarizes the methodology and the results of the preliminary **dependability studies** carried out on the SDEC solution.

Indeed, this new technology raises several questions, and its acceptability partly relies on our capacity to provide evidence that the related risks are under control.

These risks are addressed and evaluated through this dependability study, which aims at comparing a classical Easergy protection relay from Schneider Electric with the SDEC design, from an electrical protection perspective.

Two types of protection functions are first considered here, based on RTE's priority needs:

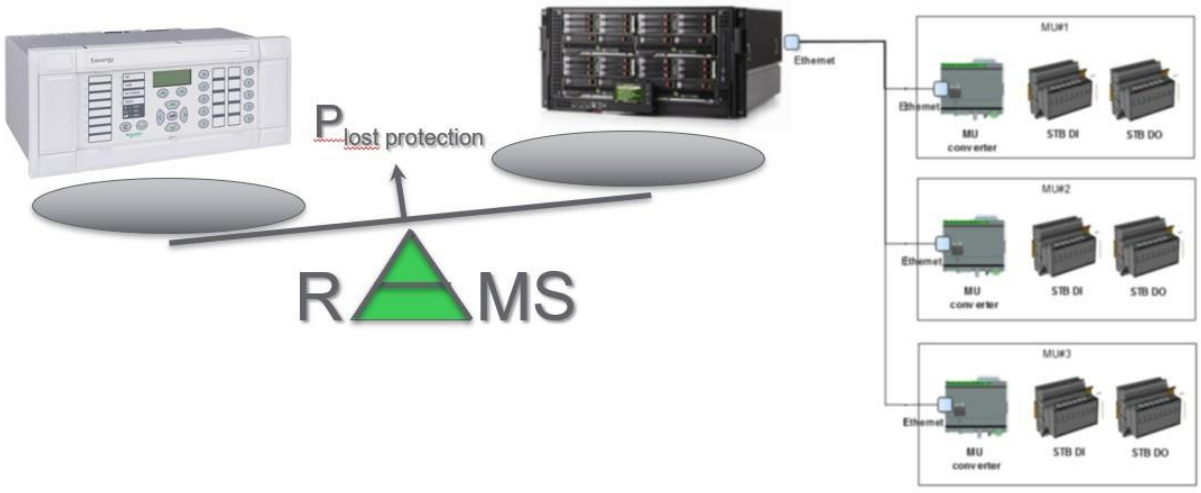
- Distant protection ANSI21, requiring both three-phase voltage and current measurements
- And the less complex overcurrent protection ANSI 50/51, current based

This study is then completed with the performance of automation functions ANSI 25 and ANSI 79 functions in an SDEC approach versus the classical implementation of these functions on a Micom C264 calculator from Schneider Electric.

The dependability metrics studied are those reflecting the customer's questions:

- Distant protection ANSI21, requiring both three-phase voltage and current measurements
- *"how often will the protection trip unduly ?* ➔ this will be measured by the **frequency of spurious actuation** of the ANSI function
- *"what is the risk that it does not trip with an electrical fault such as overcurrent ?"* ➔ this will be measured by the mean **unavailability** of the ANSI function ("masking" of the protection)

In the end, the study shall enable to **compare the risks** of spurious action or loss of the function, for a single **Easergy relay vs the SDEC solution**:



Another benefit will be to understand the differences, identify the main contributors to the risks and possibly identify potential tracks of improvement.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.3 Dependability of the protection function ANSI 21

3.3.1 Methodology

The methodology used to perform this dependability analysis is very classic in Reliability Availability Maintainability (RAM) engineering.

It consists basically in 3 main steps listed below:

1. Gather the detailed documentation related to the Proof of Concept (POC) RTE implementation
   - Global sketch of the solution / equipment used
   - BoM + detailed schematics of Schneider Electric electronics

     CT /VT (current/voltage transformers) boxes interfacing the current or voltage sensors

     Merging Unit

     STB DI (Smart Terminal Block Digital Input) used to collect status information or commands

     STB DO (Smart Terminal Block Digital Output) connected to the breaker's tripping coil
   - Detailed description + RAM Analysis of the Titanium[7] server (WindRiver)

2. Carry-out thorough RAM analyses on each part of the system
   - Reliability predictions (generic IEC 62380 models used as reference, see [9] 3.7.2 Reference documents)
   - Electronic cards Failure Modes & Effects Analysis (FMEA) ➔ failure modes? effects? detection? possible mitigation mechanisms?
   - Edge server system FMEA ➔ failure modes? effects? detection? reconfiguration?

3. Aggregate the results to build a RAM model for the global SDEC solution
   - Model the complete loop from CT/VT boxes up to Titanium server, down to the circuit breaker tripping coil
   - Electronic (frequency of spurious actuation, Pmasking=undetected failures) calculation ➔ comparison with standard Easergy Fusion v1 protection relay
   - Weaknesses identification ➔ possible improvements?

Each of the steps described above is detailed below in a specific section.

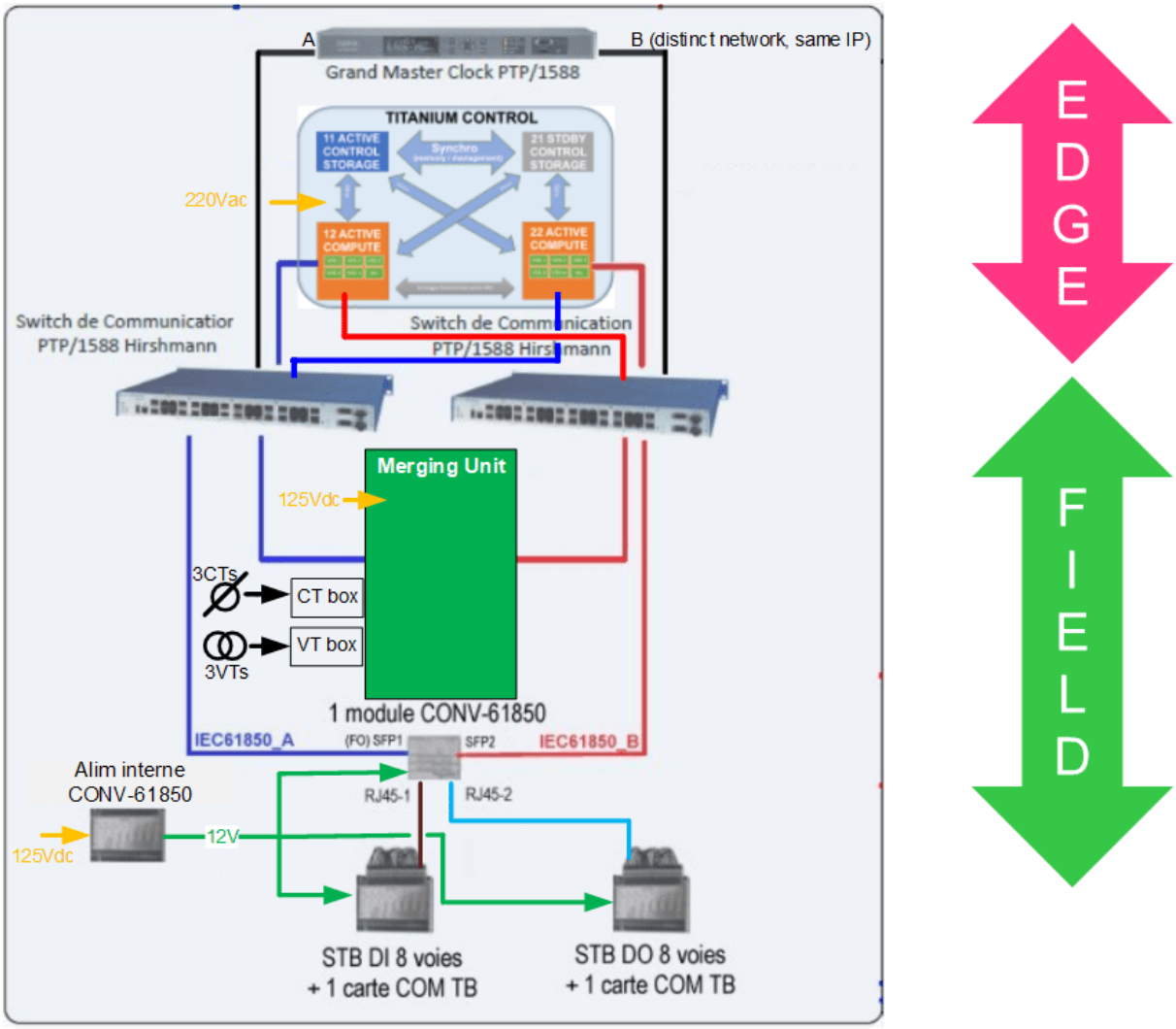
[7] Wind River Titanium Server is a software solution that includes the critical run-time components and lifecycle development tools, services, and developer support needed to successfully build and deploy a virtualized network running virtual network functions (VNF.)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.3.2 Step 1: detailed system configuration

Global sketch of SDEC implementation

The SDEC solution, as implemented in the POC RTE, is described below:



This picture shows:

- The field equipment, which

  sends current and voltage IEC61850 samples values from the CT/VT line feeders to the Titanium located at the Edge level,

  sends digital status information to the Edge as well,

  and receive commands from the Titanium, to actuate the field switchgear in return.

- The fault tolerant architecture of the Titanium, with

  redundant ”Compute” (CPT)servers hosting the virtual machines with their protection algorithms

  redundant “Control” (CTL) servers ensuring failure detection, Titanium reconfiguration and context data storage.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

List of equipment used

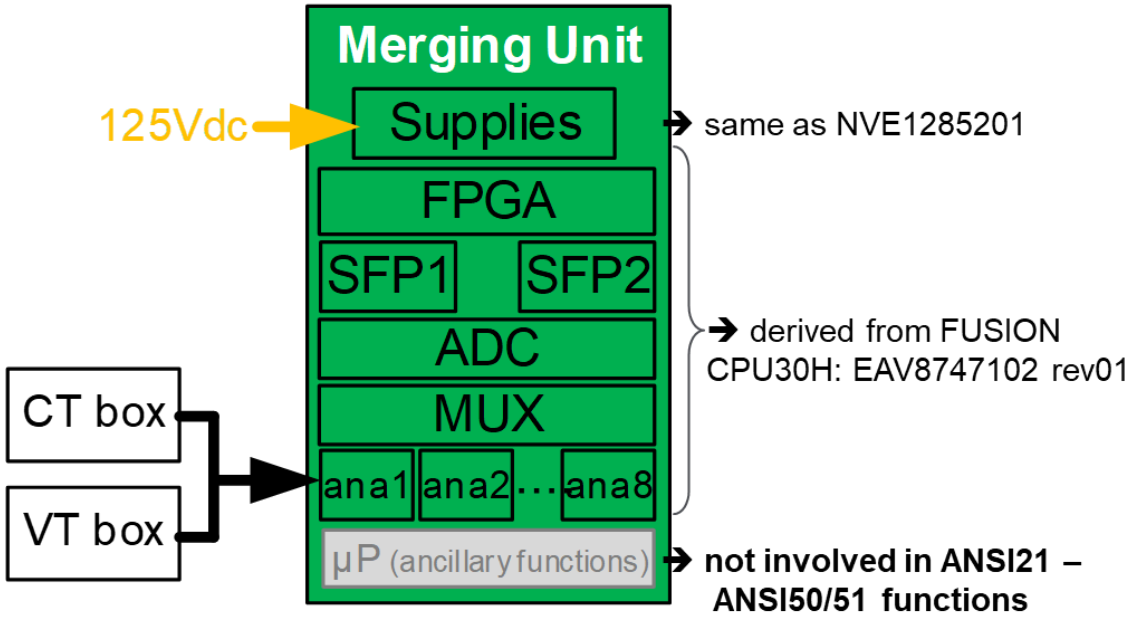
The BOM of the SDEC includes the following:

- STB DI: NHA8953920 rev02 (See [1] 3.7.2 Reference documents)
- STB DO: NHA8954118 rev00 (See [2] 3.7.2 Reference documents)
- Power supplies CEI61850 converter: NVE1285201 rev02 (See [4] 3.7.2 Reference documents)
- Merging Unit power supplies: same as CEI61850 supplies
- CEI61850 converter: QGH4421323 rev01 (See [3] 3.7.2 Reference documents)
- COM_TB module (for STB controls): NHA8954220 rev03 (See [5] 3.7.2 Reference documents)
- CT/VT module: MU_SB SCH rev01 sept.15 (See [6] 3.7.2 Reference documents)
- Titanium server: fault tolerant architecture, with 2 CPT servers + 2 CTL servers
- Communication switches A & B
- Grand Master Clock for synchronization
- Merging Unit

Focus on the Merging Unit

The Merging Unit currently equipping the POC is not the ultimate one.

The study will thus be based on the design which seems the most appropriate to us, based on the following approach:



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

The main idea behind that is to use the simplest possible design to ensure the tasks related to the protection functions, and let the more complex electronics perform elaborated, but less critical functions.

Hence, this Merging Unit uses:

- Classical analog input stages, multiplexers, and ADC to perform the analog to digital conversion
- A single FPGA to control both the analog to digital conversion and the communication through redundant communication ports SFP1 and SFP2
- And a microprocessor, dedicated to enriched ancillary functions, but playing no role in the ANSI protection functions.

Every part of this Merging Unit is, in fact, a subassembly of the existing Easergy Fusion v1 protection relay. The MU study will thus be based on selected extracts of the Easergy schematics.

3.3.3 Step 2: detailed failure analysis

Assumptions for the dependability study

The dependability analysis is carried out based on the following assumptions, established with the SDEC project team.

Methodological assumptions

- No common mode failure affects redundant equipment.
- Human errors are not accounted for (most likely during servers operation / system maintenance).
- Possible troubles by an upgrade of the Operating System are not considered either.
- SDEC protections dependability is evaluated according to IEC 62380 electronics reliability models, and compared to Easergy Fusion v1 protection relay.
- The dependability parameters are evaluated during the useful lifetime of the equipment, with constant failure rates.
- Easergy Fusion v1 dependability metrics are evaluated by re-working the FUSION1 FMEAs (see [7]), according to the POC RTE implementation (no DI, one single shunt coil, …).

Operational assumptions

- The mission time considered is 1 year: This is supposedly the interval of time between two periodic proof tests of the ANSI21 electrical protections.
- The assumed repair time following failure detection (RTE) is 2 days (48h).

Functional assumptions on protection functions

- In the RTE use case, only 3 CTs are used ➔ the zero-sequence current Io is calculated by summing the 3 phase currents, no dedicated sensor.
- If a phase current measurement is lost, then Io = -I1 ➔ the phase to earth protection trips (its setting is generally << In).
- The synchronization by the Grand Master Clock is needed only for differential protections and for the synchro-check function ➔ its loss does not impact ANSI21 nor ANSI50/51 protections.
- The ANSI21 function is assumed based on impedance measurement ➔ trips when the impedance Z becomes too low, with Z=U/I.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- Some failures of electronics impact the gain of both voltage and current measurements ➔ one conservatively considers them as protection masking failures (UE2 “failure to trip” being the most critical event in RTE application).
- Failures causing a voltage signal Ui to be stuck at a DC supply are supposed to cause a spurious ANSI21 tripping.
- 2 different scenarios are considered for the analysis:

  Scenario 1: upon failure detection, only an alarm is raised, and the system does not trip the ANSI21 protection,

  Scenario 2: upon failure detection of a non-redundant equipment, a trip command is sent to the breaker shunt coil (when possible).

Data acquisition assumptions

- The Merging Unit is built as described in section 3.3.2 and the µP embedded for advanced functions is not involved in the electrical protection functions.
- The MU power supplies are assumed similar to the STB supplies (embedded in the CONV_61850 communication STB).
- The following configuration is considered for RTE use case:

  HV circuit breaker equipped with a single shunt opening release,

  no DI is used for the electrical protections (the status of the switchgears is only used for automation functions and status display, not for ANSI21 nor ANSI50/51).

Titanium characteristics

- The basic failure rate considered for any server in the Titanium is 2,63E-06h (based on the Tellcordia MTTF prediction sent by Dell : 380 442 h @30°C GB).
- The diagnostic coverage of any server in the Titanium is supposed equal to 99% (source : KerrNet RAM study [8]).
- The remaining 1% of undetected failures of a server is assumed to be equally shared between safe and unsafe type ➔ 0,5% spurious actuation + 0,5% protection masking.
- The Titanium reconfiguration upon failure detection is as described in the Titanium FMEA (see § 0).
- Deny of service is assumed to be 1% of the communication switches failures.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Failure Mode & Effects Analyses

Failure Mode and Effects (FMEA) table template

As mentioned above, most of the FMEAs performed are related to electronic equipment and follow the steps below:

- Identify each equipment and its role;
- List all different failures that can occur on it and analyses its effects on the equipment and the global system;
- Specify how can this failure be detected.

These FMEAs are derived from those established in the scope of Easergy Fusion v1 development, see reference document [7] (3.7.2 Reference documents).

So, the same basic FMEA template was used, with the addition of new columns specific to the POC RTE use case.

This FMEA template is shown in Appendix 3.7, for illustration purpose.

List of FMEAs established

This section only lists the different FMEA tables established, and their size.

Almost 2000 lines of FMEA have been established / updated, which is the reason why these detailed documents are not included in this dependability report.

FMEA file	Size
STB DO FMEA	24 rows
CT/VT module FMEA	24 rows
Power supplies CEI61850 converter FMEA	100 rows
CEI61850 converter FMEA	112 rows
COM_TB module (STB controls) FMEA	97 rows
Merging Unit FMEA	813 rows
Titanium server FMEA	16 rows
FUSION FMEA	805 rows

***Notes** :*

1. *no FMEA has been carried out on the STB DI module, as no DI is used in our study case (distance & overcurrent protections only require analogue measurements)*
2. *no detailed FMEA has been made on the communication switches A & B either: their failures have been addressed in a worst-case approach, i.e. any failure is assumed to cause the complete loss of the switch.*

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Titanium Edge FMEA

The Titanium has already been studied in a dedicated RAM study, see [8] (3.7.2 Reference documents).

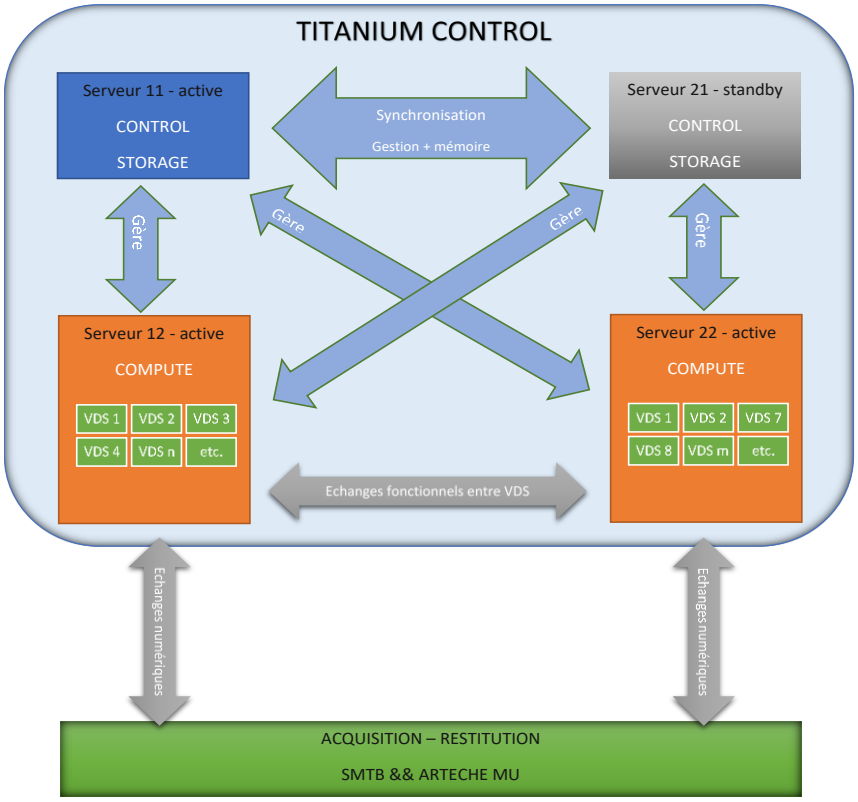
But this RAM study cannot be used straight away, as:

- The Titanium architecture studied is the common solution used by Telecommunication / Internet Service Providers, which differs from the simplified architecture used in the POC RTE
- The critical events studied in this RAM report do not include service outages lasting less than 10 seconds, which are acceptable in this kind of application.

This RAM study is nevertheless useful to understand the respective role of each compute and control server.

A FMEA was performed on the Titanium architecture used in the POC RTE, and is shown below as:

- The Titanium plays an important role in the execution of the studied ANSI21 protection functions
- And this FMEA is quite short, because the failure modes considered for each server are macroscopic.



See 4.2.1 Titanium FMEA table for details.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.3.4 Step 3: ANSI 50/51 and 21 fault tree analysis

Based on the analyses performed in the previous steps, a complete model can be elaborated for the SDEC solution, and for the Easergy relay as well.

The SDEC fault analysis is detailed in appendix 4.2.2.

3.3.5 Results of the dependability study

Initial results analysis

The results of the dependability study, under the assumptions listed above and for the scenario 1, are the following:

Scenario 1 (DD failures => alarm)	unavailability* of ANSI 50/51	F (spurious actuation of ANSI 50/51) /h	unavailability* of ANSI 21	F (spurious actuation of ANSI 21) /h
SDEC	1,75E-04	3,00E-07	1,83E-04	3,23E-07
Easergy	1,13E-03	3,85E-07	8,76E-04	3,85E-07

These results deserve the following comments:

- The mean unavailability of the distant protection ANSI21 is around 1h 36mn per year for SDEC solution. So, the probability of correct behaviour of this protection at any time is almost 99,99%
- The two solutions lead to very close frequencies of spurious trips: the gap between them is quite negligible
- The virtualized SDEC solution is almost 5 times more available than the Easergy Fusion1, evaluated on the same reliability predictive models
- This difference can be explained as follows: despite its increased complexity, the SDEC solution is more fault tolerant than the “all in one” protection relay. In particular, Easergy’s single and reliable µP performing the protection calculations is replaced by less reliable, more complex but redundant and replaceable compute servers.
- It is a good engineering practice to secure these preliminary conclusions through sensitivity studies, evaluating the impact of critical parameters changes. This is the aim of the next section.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Sensitivity studies

The sensitivity studies presented below aim at checking the influence of possible deviations in our assumption, and make sure that the hierarchy between the two solutions is not changed.

In order to keep the report concise, the results are presented only for the most critical and complex ANSI 21 function. Only one parameter is changed at a time in the FTA models.

Impact of servers' reliability

The table below sums up the effects of changes in the servers MTTF:

	λ_{server} Dell 2,63E-6/h	λ_{server} x2	λ_{server} x3	λ_{server} x5
SDEC: unavailability of ANSI 21	1,83E-04	2,41E-04	2,99E-04	4,15E-04
Easergy Fusion1: unavailability of ANSI 21	8,76E-04			

Decreasing the servers' reliability by a factor of 5 does not change the conclusion: the SDEC solution remains twice more available than the Easergy Fusion 1 relay.

Impact of operation strategy

These tables enable to compare the scenario 1 vs the scenario 2, in terms of protection functions availability:

	Scenario 1 (DD Failures -> alarm)				**Scenario 2 (DD Failures -> trip)**			
	Unavailability of ANSI 50/51	**F (spurious actuation of ANSI 50/51) /h**	**Unavailability of ANSI 21**	**F (spurious actuation of ANSI 21) /h**	**Unavailability of ANSI 50/51**	**F (spurious actuation of ANSI 50/51) /h**	**Unavailability of ANSI 21**	**F (spurious actuation of ANSI 21) /h**
SDEC	1,75E-04	3,00E-07	1,83E-04	3,23E-07	1,48E-04	8,61E-07	1,48E-04	1,07E-07
Easergy	1,13E-03	3,85E-07	8,76E-04	3,85E-07	1,11E-03	8,63E-07	8,54E-04	8,41E-07

The scenario 2 does not seem to be a good option:

- It increases the spurious trips of distance protection by a factor of 3
- But only generates a minor reduction of the protection unavailability (- 19%).

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Impact of proof tests interval

Reducing the frequency of the periodic checking of the electrical protections ANSI21 degrades their availability, for both solutions:

	Tproof = 1 year	Tproof = 2 years	Tproof = 3 years
SDEC: unavailability of ANSI 21	1,83E-04	3,01E-04	4,18E-04
Easergy Fusion1: unavailability of ANSI 21	8,76E-04	1,71E-03	2,54E-03

The SDEC solution is less affected than the Easergy relay by an increase of the period between proof tests: for a three years periodicity, SDEC is 6 times more available than Easergy Fusion v1.

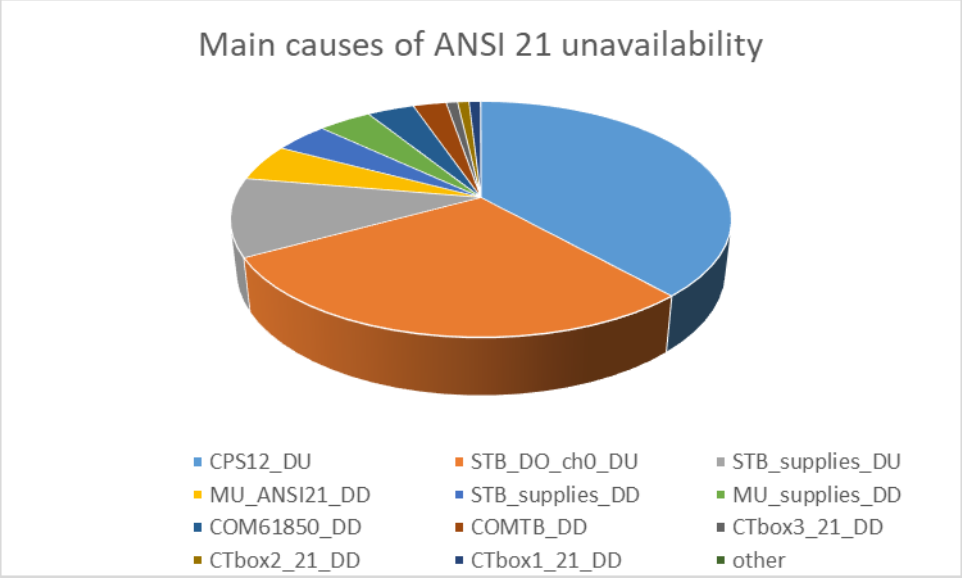
Impact of (customer dependent) repair times

	MTTR 24h	MTTR 48h	MTTR 168h
SDEC: unavailability of ANSI 21	1,50E-04	1,83E-04	3,46E-04
Easergy Fusion1: unavailability of ANSI 21	8,55E-04	8,76E-04	9,79E-04

Increasing the repair time reduces the gap between SDEC et Easergy options, but even with a one week repair time, the virtualized solution remains 3 times more available than the IED.

Impact of Titanium architecture

The analysis of the main contributors to SDEC unavailability shows that a predominant failure is the undetected failure of the active "Compute" server, which weights around 40% of the global figure:



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Indeed, the Titanium hardware is redundant but the transfers from one server to another can only be launched upon failure detection. So, an undetected failure cannot be circumvented by switching to the backup equipment.

This questions the interest of the Titanium architecture, and deserves some additional investigations with some possible variants at the Edge level.

The possible alternatives lead to the following results:

	Easergy Fusion1	SDEC Titanium	SDEC with a single CPS	2 CPS + 2 DO channels in 1oo2
unavailability of ANSI 21	8,76E-04	1,83E-04	3,08E-04	1,25E-04

This table shows the benefits of the redundant Titanium, and the possibility to improve the protection functions availability by simply using 2 independent CPS operating in 1oo2 mode. But this last solution would also double the frequency of spurious trips.

Impact of Software errors

Context

The risks generated by the new SDEC architecture are not only related to the random HW failures, but also include the effects of possible errors affecting the software.

The SW is in fact perceived as a threat by many people interested in virtualized architectures.

In the preliminary RAM study performed on the Titanium (see [8]), KerrNet Consulting made an attempt to consider the software errors in the probabilistic evaluations.

RTE technical experts would like to deploy the same approach on this dependability analysis, despite the theoretical limits of such a process (see next section).

Preliminary warning

It is important to recall that today, there is no recognized, practicable method in the RAM state of the art to quantify the risks related to SW.

For instance :

- The IEC 61508, which is the reference standard for Functional Safety management, proposes a purely qualitative approach for the software. Tables listing good practices enable to justify the confidence that can be granted to a SW, in terms of systematic errors avoidance. The recommended methods may include some metrics, such as the diagnostic coverage. But the standard does not propose any way to evaluate the SW with a failure rate.
- The French IDMR (Institute for Risks Management, formerly ISdF Dependability Institute) published a synthesis of the current state of the art in terms of software risks management. In the document IMDR GTR63 “Approach and methods for SW dependability” (ref. [10]), a complete overview is presented. Here are some major points highlighted in this document:

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

" Any association of ideas, by reference to the material, can only confuse people's minds.

Here there is no component failure, in the sense of the transition of this component from a state of good operation condition to a faulty state.

Software failures cannot be treated in the same way as hardware failures. Where hardware failures are random, software failures are systematic. If their manifestation depends on the use of the software, the introduction of their cause depends above all on human activities :

…. Nevertheless, as seen above, it is nowadays impossible to set a failure rate for the software, unless it has been shown to be free of anomalies during a period of operation that is incompatible with operating requirements. This is why the notions of degree of confidence are favoured in the different sectors of activity, compared to the notions of intrinsic reliability.

… Current standards and norms assume that it is difficult to quantify a probability of software failure, and therefore favour a qualitative approach.

… Models to quantify the reliability of software are generally seldom used because, although they can help in the analysis of the predictable behaviour of software, most of the assumptions on which they are based are subject to debate. Moreover, the results are not very significant with regard to the limits of their use. "

➔ As software bugs lead to systematic errors when a faulty SW branch is run, the behaviour is quite different to that of HW failures and can simply not be modelled by an hourly failure rate.

"KerrNet-like" modelling

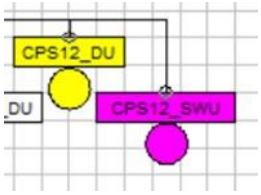
Despite the above-mentioned warning, this section presents an attempt to address SW errors in our dependability study, based on KerrNet Consulting's approach.

- The potential impacts of SW errors in our ANSI 21 application could be seen as follows:
  - **Errors could possibly affect the electrical protection algorithms, leading either to spurious trips or to inoperative protections. It is important to notice that.**
    - ✓ These protection algorithms are well proven and very stable. Unlike in most internet applications, there is no additional functionality added over the years, and the target is really to keep this qualified SW unchanged over decades.
    - ✓ These algorithms are exactly the same, in Easergy IED and in the VMs used in SDEC solution ➔ so, the risks related to protection algorithm errors are exactly the same in both solutions.
    - ✓ Therefore, this application software is a common, not discriminating part when comparing the two solutions ➔ it is useless to address it in this section.
  - **Another SW is the Titanium control algorithms, which could possibly cause spurious reconfigurations or an inability to recover upon a server failure ➔ this SW is SDEC specific, and could possibly raise additional risks for the SDEC solution**

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- Hypothetic SW errors are considered as follows in Titanium RAM study (cf. [8]):
  - **They are accounted for as HW random failures, with an hourly failure rate (/h)**
  - **This SW failure rate is based on a KerrNet custom model, based on telecom field data**
  - **λSW = f(SW size, upgrades size & frequency, process maturity level), but the equation is not detailed in KerrNet's RAM report**
  - **λSW = 1,12E-5/h (compute) to 1,34E-5/h (control servers)**
  - **KerrNet assumes that 95% of the SW faults are detected**
  - **Detected SW faults cause a remote controlled system restoration within 20mn**
  - **SW upgrades are assumed to occur once a year, to last 20mn per server.**

- So, the following assumptions can be considered to achieve a "KerrNet-like" modelling of SW errors in our FTA:
  - **VM algorithms, common to both SDEC and Easergy, are out of solutions comparison scope**
  - **Titanium control algorithms: assumed sw ~ 1E-05/h for each server**
  - **95% of SW faults are detected ➔ server unavailable for 20mn (manual restoration) ➔ λSW_D**
  - **5% of SW faults not detected ➔ server lost, no detection until server solicitation ➔ λSW_U**
  - **λSW_D and λSW_U are added in the model, for each server, in addition to the existing HW random failures**

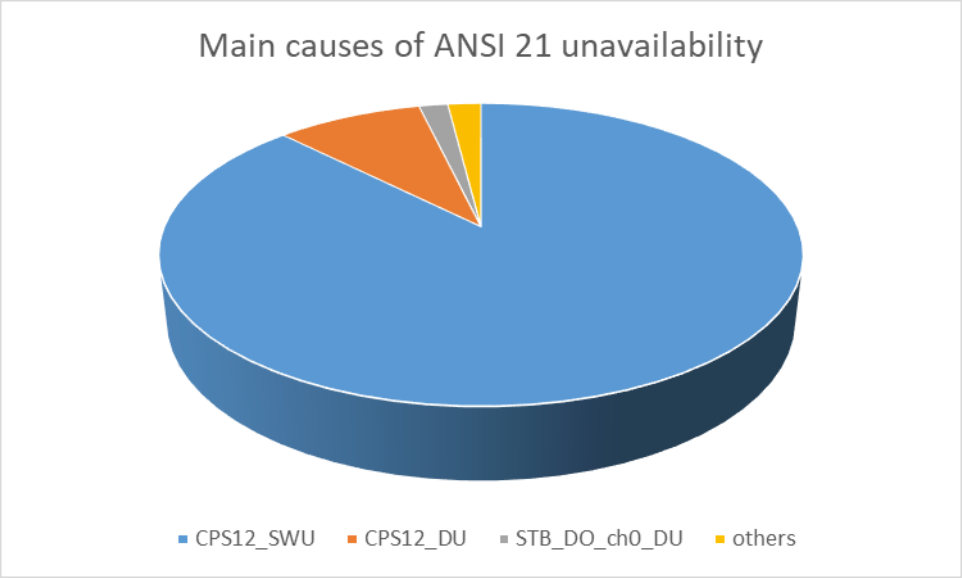


This approach leads to the following results for the distance protection unavailability (other conditions unchanged vs original simulations):

Easergy Fusion1	8,76E-04	478%
SDEC HW failures	1,83E-04	100%
SDEC HW failures + SW faults (95% detected)	2,37E-03	1292%

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

With their poor “reliability” figures and a 95% detection rate, the SW faults add a drastic contribution to the risks of ANSI 21 protection unavailability, causing the SDEC solution to become twice worse than the Easergy relay:



The 95% detection rate seems quite low to our SW experts. Increasing it to 99% leads to the following results:

SDEC HW failures + SW faults (99% detected)	6,21E-04	339%

SDEC HW failures + SW faults (99% detected)	**6,21E-04**	**339%**

Under these less pessimistic assumptions, the SDEC once again becomes better than the Easergy relay.

The reader should nevertheless keep in mind that this way of modelling the SW is not academic, so these figures both lack confidence and justification. They can be used to compare SDEC and Easergy solutions but shouldn’t be considered as an accurate value for total failure rate estimation.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.3.6 Conclusions for distance protection ANSI 21

This preliminary hardware dependability study only covers the scope of overcurrent and distance protections performed by a single breaker equipped with a shunt coil.

The SDEC solution is quite **equivalent to a classical IED in terms of spurious trip.**

It also makes the protection functions **noticeably more available than the Easergy relay** (and this conclusion is robust vs. the servers' reliability figures).

Changing the repair time or the proof tests interval does not change this hierarchy.

The optimal strategy is to simply warn the operator in case of failure detection, and not to systematically trip in such situation.

The SDEC performance could even be improved by simply using two "Compute" servers in 1oo2, without transfer mechanism. But this would double the spurious trip frequency.

The bugs possibly affecting the SW could seriously impact the SDEC performance, with a major influence of the fault detection rate. But what can easily be understood from a qualitative viewpoint is difficult to prove quantitatively, as the KerrNet approach used above is not a recognized one.

Last but not least, this study should be extended from a "product vs product" viewpoint to a "system" viewpoint: it would be interesting to evaluate, in particular, the configuration where a single Titanium manages all the protections in an HV substation, including the main and backup protections.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.4 ANSI 25 and ANSI 79 functions - Reminder

3.4.1 ANSI 25 Synchro-check basics

The Synchro-check function aims at preventing the closing of a circuit breaker if appropriate conditions are not met, in particular in case of differential voltage between its sides. Such a voltage difference can occur in case of:

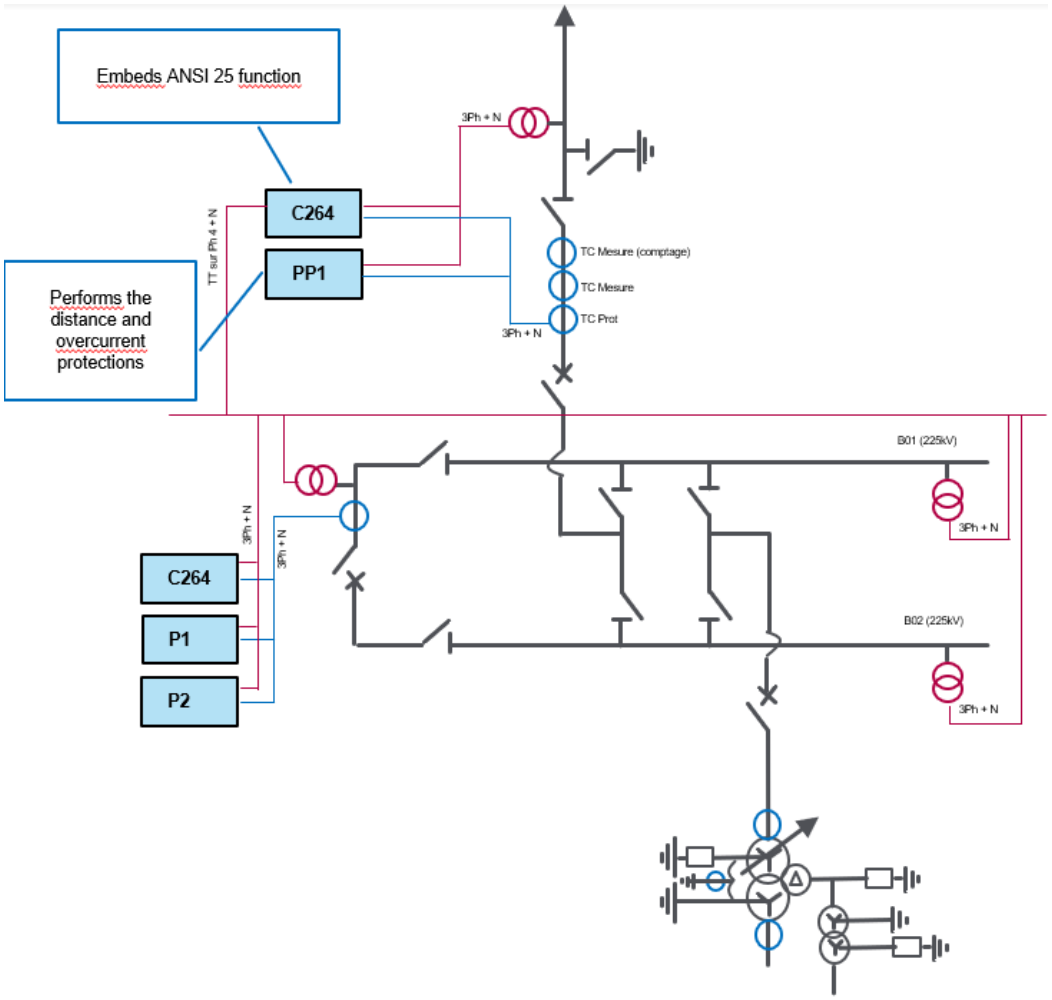
- Voltage amplitude gap between the upstream and downstream supplies
- And/or frequency difference at each side of the breaker
- And/or phase shifting between upstream and downstream sources

The coupling is allowed only if all conditions are met: voltages, frequencies and phase shift must be within the acceptable range.

3.4.2 ANSI 25 "classical" implementation

In its current implementation, the ANSI 25 function is performed by a C264 controller, monitoring and analysing voltages at both sides of the breaker, and performing the automation algorithm.

As is shown below, this controller manages the breaker closing inhibition, while the current-based protection functions (e.g. ANSI 50/51, ANSI 21…) are supported by an independent MICOM protection relay (e.g. PP1).



Only one phase voltage is measured at the busbar level (B01 or B02 above), and the coupling conditions are checked by analyzing the busbar phase 1 voltage measurement and the line phase 1 voltage acquisition.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.4.3 ANSI 25 virtualization

The following sketch depicts the synchro-check implementation with the virtualized solution.

This scheme shows the complete virtualization of protection (overcurrent, distance, ...) as well as automation (synchro-check, auto-recloser,...) functions.

The basics remain the same, with:

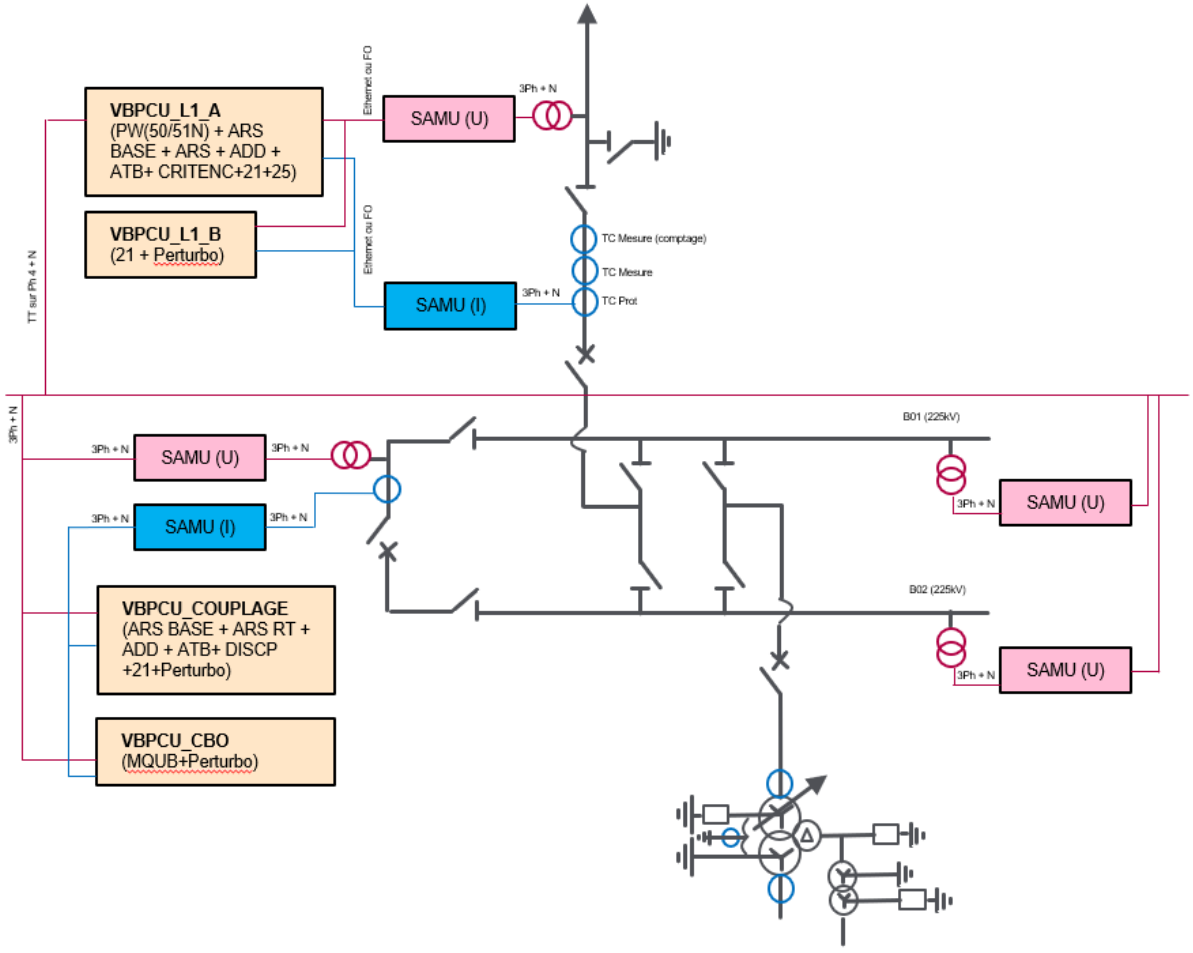
- Field equipment limited to

  VT connection boxes

  SAMU merging units

  IEC 61 850 communication devices controlling STB-DO terminal boxes controlling the HV switchgear operation

- And complex treatments such as electrical protections and automation algorithms managed at edge level, by redundant Compute Servers.



On the above scheme, SAMU devices are shown in blue when they deal with current measurements, and in pink when they perform voltage acquisition:

- SAMU (I) provide current samples to perform ANSI 50/51 and ANSI 21 protection functions at edge level
- while SAMU (U) merging units send voltage samples to servers performing the ANSI 25 function and/or other protection algorithms such as ANSI 21. The same principle is used to check the coupling conditions: the busbar phase 1 voltage measurement is compared with the line phase 1 voltage acquisition.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.4.4 ANSI 79 Auto-recloser basics

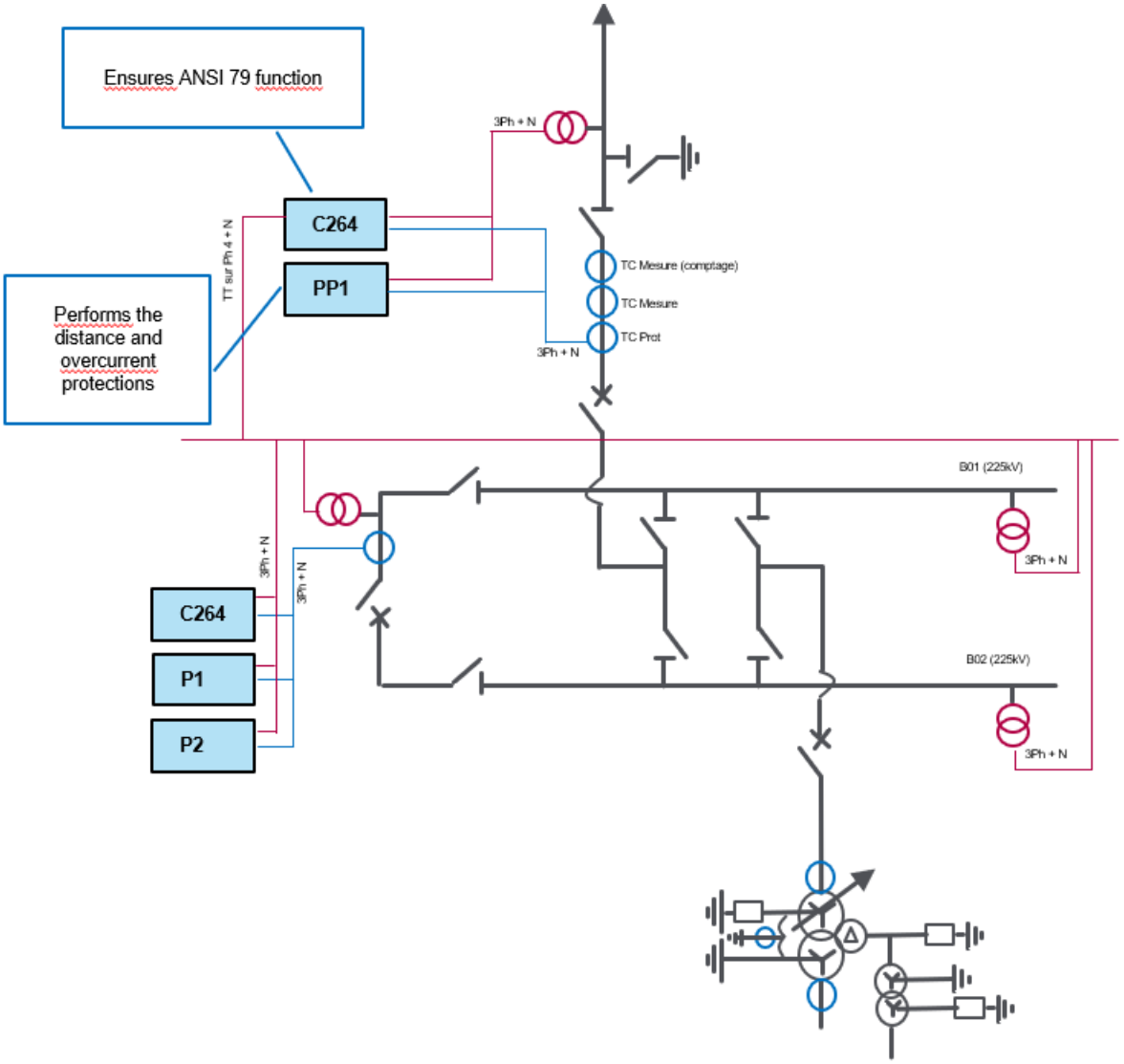
The auto-recloser is an automation function used to limit the down time after tripping due to transient or semi-permanent faults on overhead lines.

A recloser orders automatic reclosing of the circuit breaker after the time delay required to restore the insulation has elapsed. Its operation is easy to adapt for different operating modes by parameter setting (number of reclosing cycles, delays, etc…).

In the majority of fault incidents, if the faulty line is immediately tripped out, and time is allowed for the fault arc to de-ionize, the reclosure of the circuit breakers will result in the line being successfully re-energized.

3.4.5 ANSI 79 "classical" implementation

As is the case for the ANSI 25 function, the recloser function ANSI 79 is currently performed by a C264 controller, receiving tripping commands from independent protection relays (e.g. PP1) and managing the reclosing sequence according to the defined settings.



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

The recloser function uses two digital inputs:

- An information received (by Goose or wired link) from the protection relay, indicating that a tripping order was sent to the breaker
- Plus an information indicating that the breaker is open.

If both conditions are true, it launches the breaker reclosing sequences according to its settings.

3.4.6 ANSI 79 virtualization

The global sketch of the recloser virtualized implementation is the same as the synchro-check scheme.

- Protection functions (ANSI 50/51, ANSI 21, ANSI 25…) as well as automation functions (ANSI 79) are treated by redundant edge servers
- These servers are using digital signals received from the field-installed STB-DIs.

In the virtualized solution, please note that all the protection functions are performed by the edge compute servers. So, the information “protection tripped’’ is already available at edge level, and does not need to be acquired from the field. This simplifies the function and avoids the risks of failure to transmit the tripping orders from the field protection relays to the automation controller.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.5 Dependability study for ANSI 25 and 79

3.5.1 Target

The aim of this dependability is, again, to compare the conventional, field-equipment based solution with the more centralized, virtualized approach.

This comparison is based on the probabilistic quantification of Undesirable Events defined in the next section.

3.5.2 Critical events studied

ANSI 25 function

The Undesirable Events are chosen to reflect at best the customer's stakes. For the synchro-check function, the following criteria are proposed:

- "what is the risk that the synchro-check never allows to close the breaker ?" ➔ event UE25-1
- "what is the risk that it allows the breaker closing, even with a voltage difference between its upstream vs downstream terminals ?" ➔ event UE25-2

ANSI 79 function

The same approach leads to the following Undesirable Events for the auto-recloser function:

- "what is the risk that the function does not re-close the breaker ?" ➔ event UE79-1
- "what is the risk that the function spuriously re-closes the breaker in undue conditions ?"" ➔ event UE79-2

The study shall enable to **compare the above-listed risks** for the two possible options : **classical, C264-based implementation vs the SDEC solution.**

3.5.3 Dependability approach

This preliminary study aims at performing a quick comparison between the C264-based deployment of ANSI 25 and ANSI 79 functions and their concurrent, virtualized implementation.

In order to be as conservative as possible, the POC RTE will in fact be compared with the simplest possible implementation of the synchro-check and auto-recloser functions on an integrated controller. This simplest standalone solution will be derived from the schemes considered in the previous section. Then:

- The C264 can be only more complex than the minimalist implementation considered
- If the virtualized solution proves to be better than the minimalist controller considered, then it can only be even better than the current C264 controller.

So, the reasoning will be based on a "functional" approach, considering:

- The definition of ANSI 25 and ANSI 79 functions
- What inputs they are using
- What outputs they are involving to control an HV breaker
- What treatments they are performing
- And what are the minimum resources needed to perform these treatments.

In order to ease the comparison and make it easy to understand, both solutions will be depicted in an RBD approach, showing the functional blocks used to perform the mission.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.5.4 Assumptions

Limits of scope

- The dependability analyses only considers the functions and equipment described in section 3.4.
- Only the synchro-check and the recloser modules are analysed.

Technical assumptions

- The mission time considered is 1 year: This is supposedly the interval of time between two periodic proof tests of the system.
- The Merging Unit is supposedly built as described in [6] (3.7.2 Reference documents). An embedded µP performs advanced functions, but is not involved in the analog to digital conversion nor in the broadcasting of digitized samples of voltage or current measurements.
- As per [4] (3.7.2 Reference documents), the MU power supplies are assumed similar to the STB supplies (embedded in the CONV_61850 communication STB).
- The following configuration is considered for RTE use case:

  check is studied in the synchro- “live bar and live incomer” operating mode

  the active CPTS performs both the electrical overcurrent or distance protections and the automatic recloser function ; so, the information “breaker tripped by a protection” is already available in the server and does not need to be received from the field.
- In order to draw unbiased conclusions when comparing the two different technologies, we voluntarily ignore the software improvements that could potentially be deployed on the POC RTE, and are not embedded on the C264 controller. Hence, we suppose that both solutions share the same principles below:

  in the “live bar and live incomer” operating mode, the synchro-check enables the breaker closing only if the line voltage 1 and the bus voltage 1 are within stipulated tolerances (amplitude + frequency + phase shift)

  other measurements are not accounted for by the ANSI 25 algorithm, neither for decision making nor for fault detection.
- The dependability parameters are evaluated during the useful lifetime of the equipment, with constant failure rates.
- The failure rate of each elementary functional block is derived from the previous section on ANSI 21, by updating the equipment FMEAs to the context of ANSI 25 and ANSI 79 functions.
- The voltage samples used to perform the synchro-check function are delivered by a single Merging Unit, so that there is no risk of desynchronization in case of Grand Master Clock failure. This is possible and should be considered as a golden rule when implementing the ANSI 25 function.
- Upon failure detection:

  the synchro-check function does not enable the breaker closing

  and the recloser does not try to reclose the breaker.
- The Titanium architecture considered is based on

  3 redundant compute servers (one of them being maintenance) used as a backup only during a server

  monitored by two control & storage servers
- Its reconfiguration principles upon detected failure is as described in the Titanium FMEA (see [7] 3.7.2 Reference documents § 5.2.3)
- The basic failure rate considered for any server in the Titanium is 2,63E-06h (based on the Tellcordia MTTF prediction sent by Dell : 380 442 h @30°C GB)
- The diagnostic coverage of any server in the Titanium is supposed equal to 99% (source : KerrNet RAM study [8] (3.7.2 Reference documents))

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- The remaining 1% of undetected failures of a server is assumed to be equally shared between safe and unsafe type ➔ 0,5% spurious actuation + 0,5% protection masking
- Should the active compute server be unable to communicate with the field (both Ethernet links lost), then the Titanium automatically performs a switchover to the backup compute server
- The software errors are excluded, both for compute servers algorithms and for the system reconfiguration managed by the control servers
- The deny of service is assumed to be 1% of the communication switches failures
- The assumed repair time following failure detection (RTE) is 2 days (48h)
- No common mode failure affects redundant equipment
- Human errors are not accounted for (most likely during servers operation / system maintenance)
- Possible troubles induced by an upgrade of the Operating System are not considered either.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.5.5 Dependability analysis of the ANSI 25 function

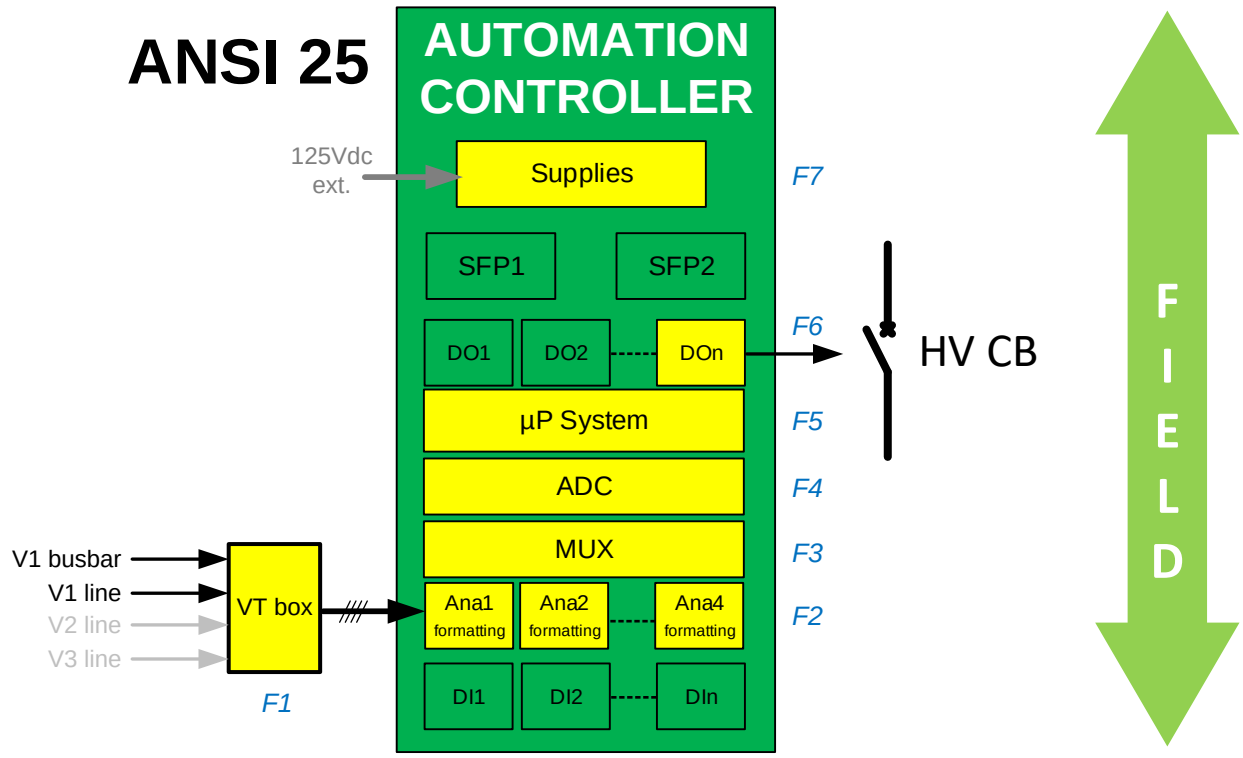
ANSI 25 qualitative analysis (RBD approach)

Classical implementation of ANSI 25

The following functions must be achieved by an integrated stand-alone controller (such as the C264) to perform the synchro-check:

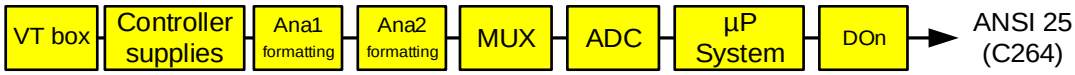
- F1: the voltage sensors (substation voltage busbar phase 1 + line phase voltages 1 to 3) must be connected to the controller.
- F2: the analog signals must be formatted (scaling, overvoltage protection,…) to be compliant with the electronic stages processing them
- F3: the analog signals shall be multiplexed to enable a single ADC to perform the analog to digital conversion
- F4: the analog signals are then converted into digital samples by an ADC
- F5: analog signal multiplexing and digital signal processing is carried out by a µP-based system
- F6: a single digital output circuit is necessary to interface the low power µP output with the HV breaker closing coil
- F7: internal supplies are necessary to convert the single input supply to various low voltage levels used by the controller internal electronics.

Hence, the simplest possible implementation of such a controller is as follows. The functional blocks shown in yellow below are those necessary to perform the synchro-check (others are shown for illustration purpose only):



Notes: - functions F1 to F7 are shown near the corresponding block
- V2 line and V3 line signals are not used by the ANSI 25 function

This leads to the following RBD for the synchro-check function:



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

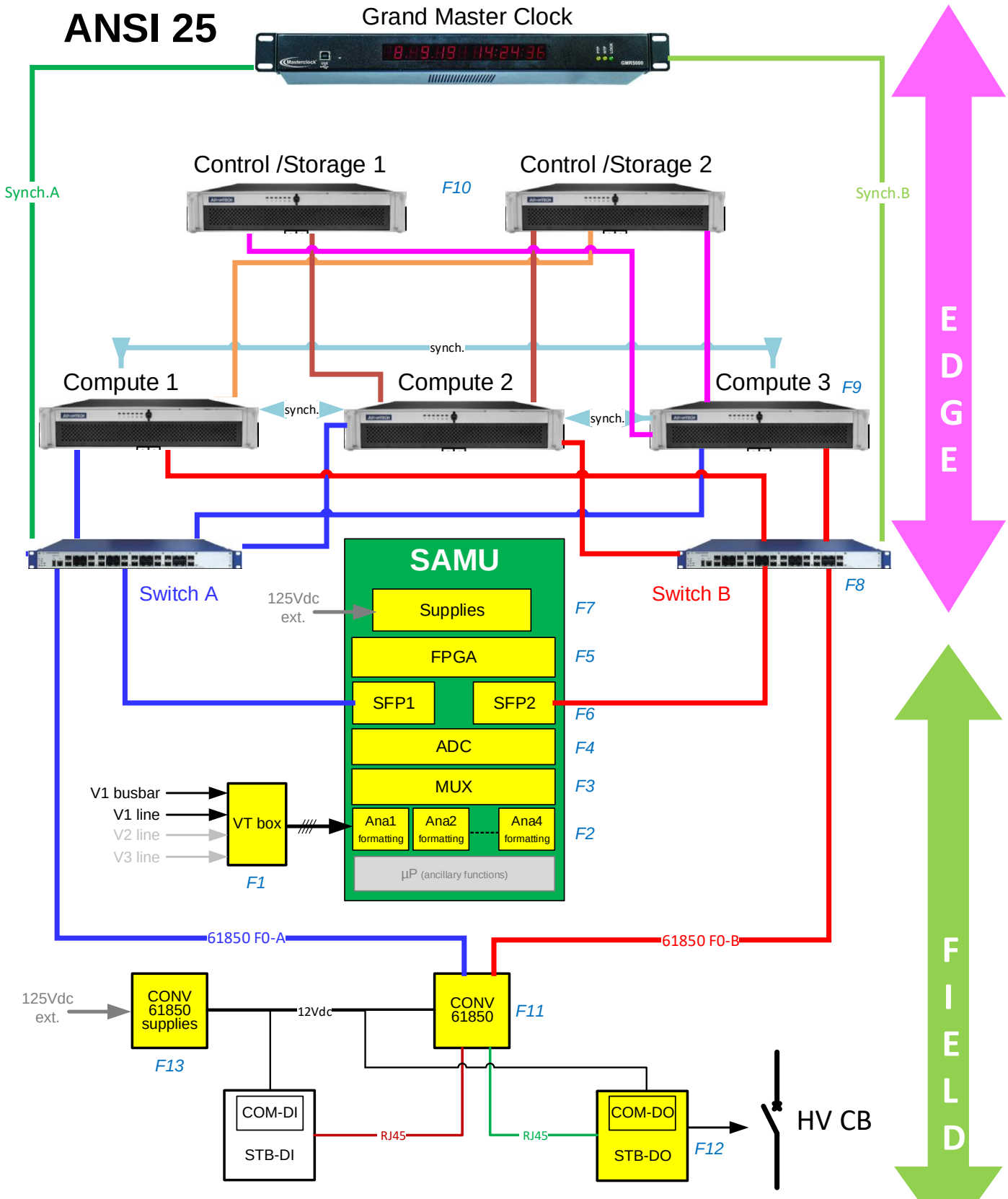
POC RTE implementation of ANSI 25

The virtualized implementation of the ANSI 25 synchro-check is based on the following elementary functions:

- F1: the voltage sensors (substation voltage busbar phase 1 + line phase voltages 1 to 3) must be connected to the SAMU
- F2: the analog signals must be formatted (scaling, overvoltage protection,…) to be compliant with the electronic stages processing them
- F3: the analog signals shall be multiplexed to enable a single ADC to perform the analog to digital conversion
- F4: the analog signals are then converted into digital samples by an ADC
- F7: internal supplies convert the single input supply to various low voltage levels used by the SAMU
- F8: redundant communication switches support the communication between the Titanium controller and the field equipment
- F9: 3 redundant compute servers (one being on hold for maintenance phases only) perform the processing of the synchro-check, with an ability to switch-over without losing the function
- F10: the switch-over between CPTS and the storage of information enabling context recovery is managed by 2 redundant control servers
- F11: messages sent redundant FO communication links to remotely control the HV breaker are treated by an IEC 61 850 converter
- F12: an STB-DO channel is used to control the breaker closing release, based on messages received from the IEC 61 850 converter
- F13: the IEC 61 850 converter and the field STBs are supplied by a single DC/DC converter.

This can be represented on the scheme shown on the next page, with the functional blocks used for ANSI 25 in yellow and the function related to each of them in blue

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276



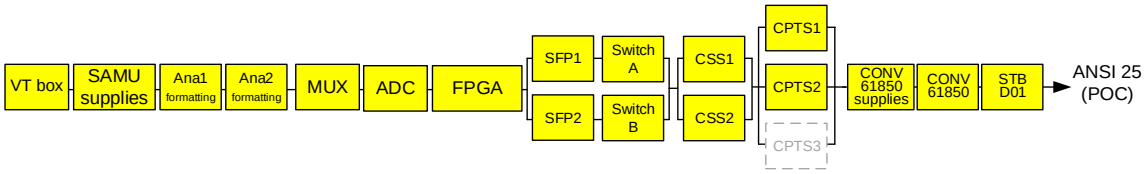
Note 1: - functions F1 to F13 are shown near the corresponding block
- V2 line and V3 line signals are not used by the ANSI 25 function

Note 2: the synchronization provided by the grand master clock is not mentioned here as a sub-function of the virtualized synchro-check. Indeed, the grand master clock aims at avoiding any time delay between samples coming from various Merging Units and involved in a same protection function. As the two

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

voltage signals necessary for the ANSI 25 can be treated by a single SAMU, such a synchronization is useless in fact.

The ANSI 25 implementation shown on the next page leads to the following RBD diagram for the virtualized synchro-check function:



Note : the compute server #3 is shown in grey dotted lines and is not considered in the analysis, due to the strategy envisaged by the operator

- in normal operation, this server is on hold and only two redundant CPTS are doing the job
- CPTS3 is used only when one of the other CPTSs must be maintained, to maintain the nominal level of performance.

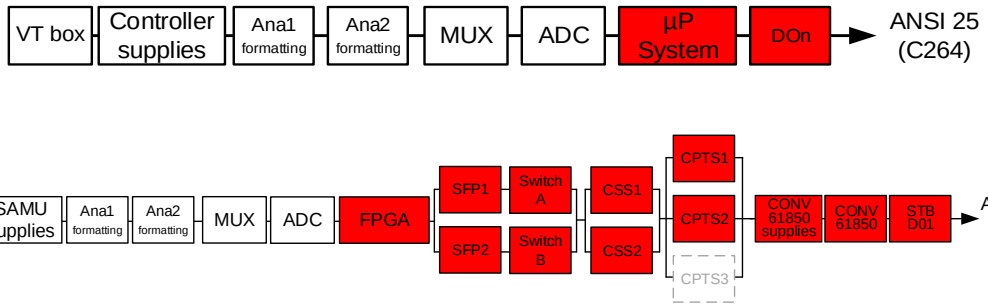
Comparison between the classical vs the virtualized ANSI 25

The RBD analyses performed above highlight that both solutions are involving some functional blocks of a similar type:

- F1: connection of the voltage sensors
- F2: the analog signals formatting
- F3: the analog signals multiplexing
- F4: the analog signals are then conversion to digital samples
- F7: generation of internal supplies

are present in both implementations, with a similar level of complexity thus similar reliability figures.

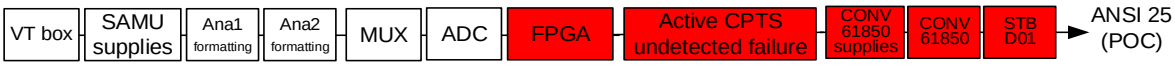
Hence, the main differences between the classical solution and the innovative SDEC are the functional blocks highlighted in red below:



Again, the challenge is mainly between an integrated µP system and a much more complex system, which less reliable equipment is redundant.

As it was shown during the ANSI 21 RAM study, the main risk with the Titanium is a potential undetected failure of the active compute server, which prevents the automatic switch-over to its backup CPTS. Hence, the equivalent RBD diagram of the POC RTE becomes:

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276



So, the situation is basically the same as for the distant protection studied, and should lead to similar conclusions: despite its inherent complexity, the virtualized solution should in the end be more reliable than the classical solution.

ANSI 25 quantitative analysis (FTA approach)

Based on the analyses performed in the previous steps, a complete model can be elaborated for the SDEC solution, and for the controller-based solution as well.

The models are based on the fault tree methodology, which enable:

- To consider multiple failure scenarios
- An easy understanding of the combinations of failures leading to each critical event studied.

The FTA models are detailed in the following sections, for both implementations of the ANSI 25.

All basic events used in the FTAs are detailed in Appendix 3.7.1 Electronics FMEA tables template, with the associated dependability parameters.

The analysis is detailed in 4.2.3.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Conclusions for the ANSI 25 function

ANSI 25	λ_{UE25-1} /h Breaker closing disabled	λ_{UE25-2} /h Breaker closing allowed
SDEC	**1,22E-06**	**2,50E-08**
Stand-alone controller	**1,13E-06**	**3,43E-08**

Only failure rates figures are shown in the table above, in order not to complexify the analysis and because they are sufficient to compare both solutions and draw conclusions.

- Globally, there is no major difference in the performance level achieved by the two technologies. The figures are very close for both the risk of disabling the coupling between well synchronized sources and the risk of enabling the coupling of unsynchronized networks.
- The risks that the synchro-check function unduly prevents the coupling is a little bit higher with the virtualized solution. This is mainly due to the fact that the SDEC implementation involves two supplies at the field level (one for the SAMU, the other for the STBs) while only one power supply (of similar complexity) is required for the stand-alone controller. Any loss of a power supply prevents from sending a closing command to the circuit breaker, hence the increased occurrence of event UE25-1 with the SDEC solution.
- On the other hand, the risks of letting the breaker close with a voltage difference between its ends is a little bit lower with the virtualized implementation of the synchro-check. This is a good point, as the event UE25-2 is probably more critical, due to its potential consequences in terms of equipment damages and HV network stability. The analysis of the **cut sets** shows the benefits of the redundant compute servers: in case of a detected failure of the active compute server, the synchro-check remains operant thanks to the backup server. The undetected failures of the active compute server put the synchro-check at risk, but the diagnostic coverage of the Titanium is very high.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.5.6 Dependability analysis of the ANSI 79 function

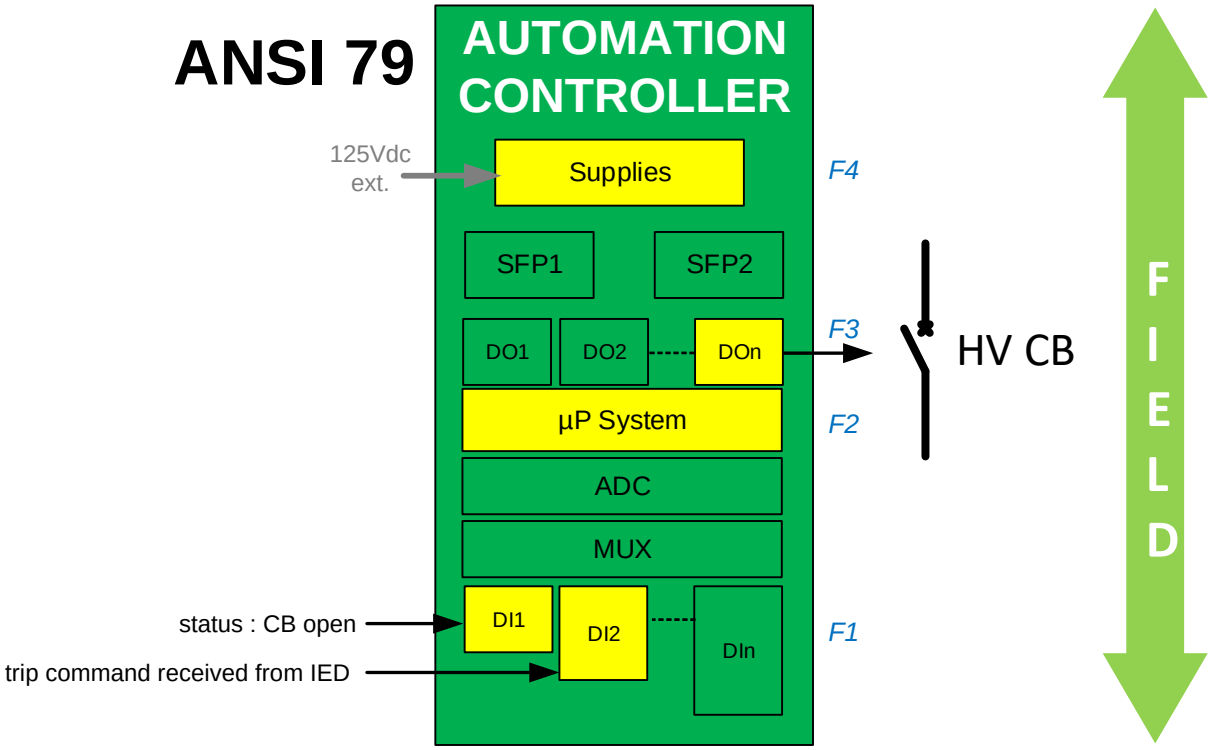
ANSI 79 qualitative analysis (RBD approach)

Classical implementation of ANSI 79

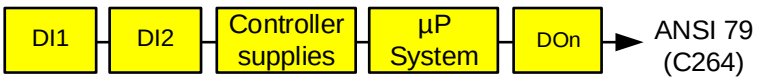
The following functions must be achieved by an integrated stand-alone controller (such as the C264) to perform the automatic recloser:

- F1: the digital signal indicating the tripping of a protection function and the HV breaker position must be acquired from field equipment.
- F2: these digital inputs are treated by a µP-based system, launching the auto-recloser sequence according to the user settings
- F3: a digital output circuit is necessary to convert the µP output into a driving command to the HV breaker closing release
- F4: the controller internal electronics must be supplied with various low voltage levels.

Hence, the simplest possible implementation of such a controller is as follows. The functional blocks shown in yellow below are those necessary to perform the auto-recloser:



This leads to the following RBD for the auto-recloser function:



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

POC RTE implementation of ANSI 79

The virtualized implementation of the ANSI 79 auto-recloser is based on the following elementary functions:

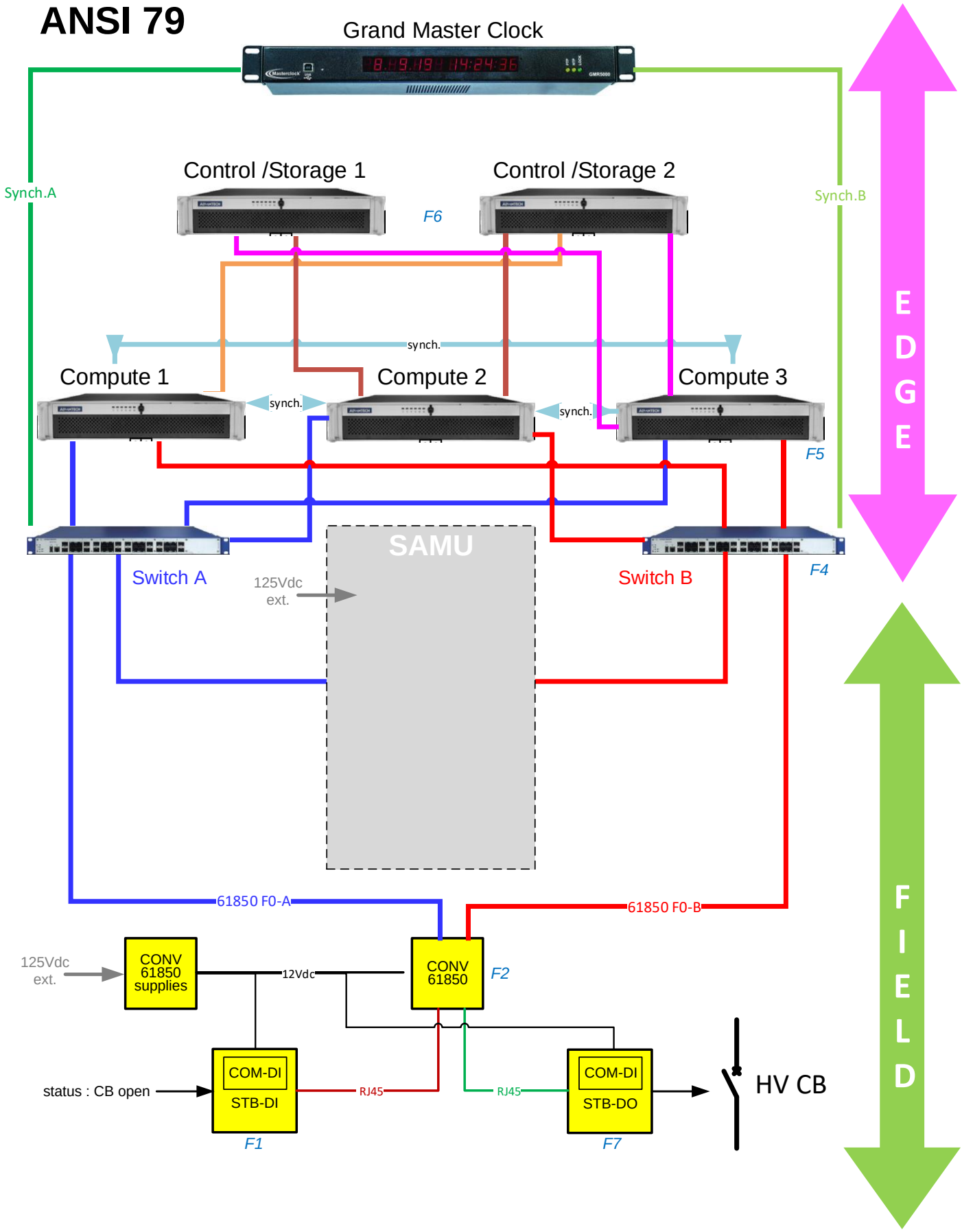
- F1: only the digital signal indicating the HV breaker position must be acquired from field equipment.
- F2: this information is sent to the EDGE by an IEC 61 850 converter through redundant FO communication links
- F3: the IEC 61 850 converter and the field STBs are supplied by a single DC/DC converter.
- F4: redundant communication switches support the communication between the Titanium controller and the field equipment
- F5: three redundant compute servers (one being on hold for maintenance phases only) perform the processing of the auto-recloser, with an ability to switch-over without losing the function
- F6: the switch-over between CPTS and the storage of information enabling context recovery is managed by two redundant control servers
- F13: an STB-DO channel is used to control the breaker closing release, based on messages received from the IEC 61 850 converter (same equipment as for F2)

This can be represented on the scheme shown on the next page.

Notes:

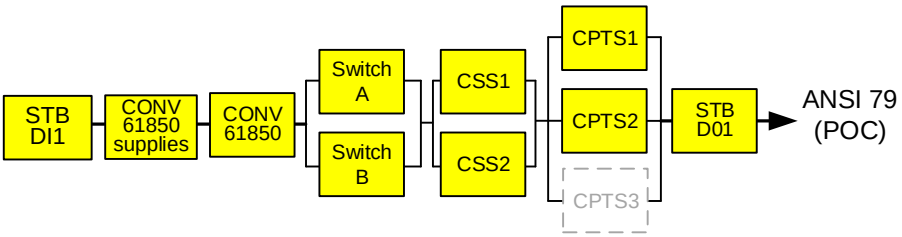
- As the auto-recloser is based on digital inputs only, the SAMU is not involved in this function
- The grand master clock is not necessary for the ANSI 79 function either
- As can be seen on the scheme, the auto-recloser only needs one single status from the field (the tripping of a protection function being managed by the Titanium, it is already known at EDGE level)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Such an implementation leads to the following RBD diagram for the virtualized auto-recloser function:



Note: the compute server #3 is shown in grey dotted lines and is not considered in the analysis, due to the strategy envisaged by the operator

- in normal operation, this server is on hold and only two redundant CPTS are doing the job
- it is used only when one of the other CPTSs must be maintained, to maintain the nominal level of performance.

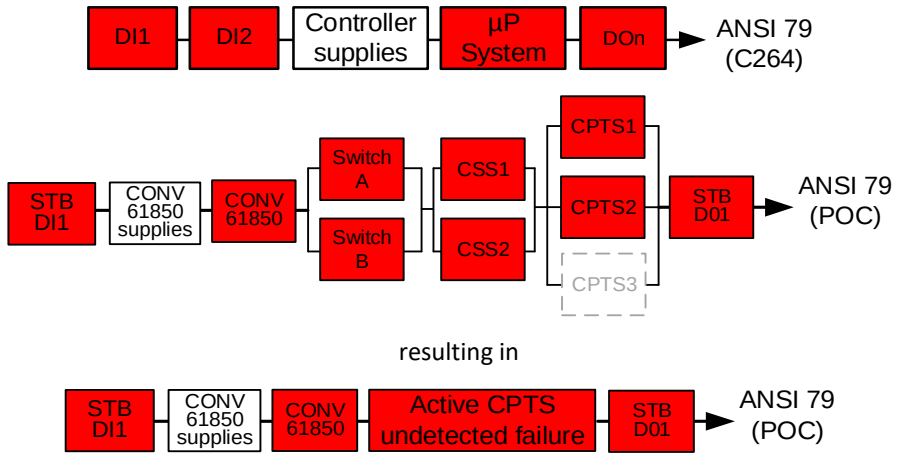
Comparison between the classical vs the virtualized ANSI 79

The RBD analyses performed above highlight that both solutions are involving some functional blocks of a similar type:

- F1: connection of the voltage sensors
- F2: the analog signals formatting
- F3: the analog signals multiplexing
- F4: the analog signals are then conversion to digital samples
- F7: generation of internal supplies

are present in both implementations, with a similar level of complexity thus similar reliability figures.

Hence, the main differences between the classical solution and the innovative SDEC are the functional blocks highlighted in red below:



So, the conclusion should be the same: thanks to its high self-diagnostic coverage, the Titanium-based solution should in the end be more reliable than the classical solution.

ANSI 79 quantitative analysis (FTA approach)

The analysis is detailed in 4.2.4.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Conclusions for the ANSI 79 function

ANSI 29	λ_{UE79-1} /h No reclosing	λ_{UE79-2} /h Spurious reclosing
SDEC	**9,94E-07**	**5,00E-08**
Stand-alone controller	**1,22E-06**	**6,48E-08**

From the above failure rates, the following conclusions apply:

- The figures are very close for both technologies, whatever the failure considered. In other words, the performance of the auto-recloser is quite similar with the classical stand-alone controller and with the SDEC system.
- The risks that the auto-recloser does not perform the CB reclosing is slightly lower with the virtualized solution. Indeed, the SDEC architecture enables to have the information of tripping command already available in the Titanium, so a single DI input can be used instead of two for the controller-based architecture. This benefits to the availability of the recloser.
- The same reason explains that the risk of spurious actuation of the auto-recloser, with conditions not met, is also lower with the virtualized implementation. Should the SDEC solution need another DI input, then the frequency of spurious auto-reclosing would be similar to the classical solution.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.5.7 Conclusions for the ANSI 25 and 79

This hardware dependability study deals with the synchro-check and the auto-recloser functions.

The quantitative analysis globally confirms what was expected following the preliminary qualitative assessment.

In order to provide conservative conclusions, the SDEC virtualized solution is compared to a generic, minimalist stand-alone controller.

Re-working the detailed electronics FMECAs performed during the study of the distance protection ANSI 21 leads to the following findings:

- The current solution and the virtualized solution share some common functional blocks with a similar reliability.

- The differences are limited to a few functional blocks, similar to those highlighted in the ANSI 21 study:
  - ✓ In the current solution, the most critical part of the loop is the µP system (controller CPU card)
  - ✓ In the virtualized system, the less reliable equipment (i.e. servers and communication devices) is redundant and the main risk is related to the non-detection of a failure affecting the active compute server, as was the case for the distance protection function.

- The quantification of the critical events confirms that both solutions offer very close performance, with:
  - ✓ The SDEC implementation, penalized by its two field power supplies (instead of one), being slightly less available in terms of synchro-check function (more spurious disabling of CB closing ER25-1);
  - ✓ But the virtualized solution slightly better than the classical controller for all other performance (events ER25-2, ER79-1 and ER79-2).

- The key points to be carefully addressed during the design of the POC RTE are:
  - ✓ To **minimize the risks of systematic errors in the software**, both at applicative level (i.e. protection algorithms must be well proven) and at Titanium level (i.e. the risks of spurious reconfigurations or failure to reconfigure on demand must be minimized),
  - ✓ To **maximize the failure detection at Titanium servers level** (built-in tests + system-level detection), so as to minimize the risks of failure to transfer on the backup compute server. For instance, the current algorithm could be improved to detect if the multiplexer is stuck on one voltage channel, which could cause the synchro-check to allow the CB closing with a voltage gap between its ends. This can be done by checking that there is a 120° phase shift between the three-line voltages measured. This does not change the figures drastically, but it contributes to secure the function even more.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3.6 Global conclusion

This study shows that **the classical IED and the SDEC implementations offer very similar performances** in terms of dependability, both for distance protection functions as well as for the synchro-check and the auto-reclosure.

In particular**, the SDEC solution** is quite **equivalent to a classical IED in terms of spurious trip.** It also makes the protection functions **noticeably more available than the classical relay.**

Those conclusions are **robust** to several factors such as e repair time, servers' reliability figures or the proof tests interval.

As software induced failures are difficult to take into account, the SDEC Proof of Concept will pay special attention to systematic errors that could undermine the global reliability. The failure detection mechanisms at Titanium servers level also plays an important role and will be closely monitored.

The results of this study are very positive and **validate the SDEC concept on several aspects:**

- The reliability for vital functions like protection;
- The reliability for automation functions like synchro-check and the auto-recloser functions;
- The validity of those conclusions with a wide range of hypothesis.

This study could be extended from a "product vs product" viewpoint to a "system" viewpoint: it would be interesting to evaluate, in particular, the configuration where a single Titanium manages all the protections and automation in an HV substation, including the main and backup protections.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4. APPENDIX

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.1 UC 10 requirements

This section contains Use Case requirements at a level of detail sufficient to enable CPS4EU designers to design components and pre-integrated architectures to satisfy those requirements, and testers to test that the system satisfies those requirements.

Throughout this section, every stated requirement will be externally perceivable by users, operators, or other external systems.

Important note: In the following requirements, the MPC optimizer is considered with a black box approach: it receives inputs and generates commands. The inner parameters of the MPC are not discussed in this document as many parameters are still under evaluation (for example cost of energy curtailment, cost of using downgraded network topologies).

4.1.1 Functional Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-FNC-01	General network situation acquisition	Every 1 minute, the NAZA acquisition shall get new network situation from upper level and transmit it to NAZA cores.	High
UC10-FNC-02	Batteries set points acquisition	Every 1 minute, the NAZA acquisition shall get new battery set-points from upper level and transmit them to NAZA cores	High
UC10-FNC-03	Generation forecast acquisition	Every 10 seconds, the NAZA acquisition shall get new generation forecasts and transmit them to NAZA cores.	Medium
UC10-FNC-04	Area network datapoints acquisition	Every 10 seconds, the NAZA acquisition shall get new datapoints and transmit them to NAZA cores.	High
UC10-FNC-05	Area events topological events acquisition	Every 1 second, the NAZA acquisition shall get new topological events and transmit them to NAZA cores.	High
UC10-FNC-06	Levers setpoints normal calculation	Every 5 seconds, the NAZA cores shall calculate levers setpoints with MPC normal algorithm.	High
UC10-FNC-07	Levers setpoints back-up calculation	Every 5 seconds, the NAZA cores shall calculate levers setpoints with back-up logigram algorithm.	High
UC10-FNC-08	Supervisor normal mode	If setpoints are calculated by NAZA Cores after 2s upon levers setpoints normal calculation (UC10-FNC-06), the supervisor shall be in normal mode.	High
UC10-FNC-09	Supervisor back-up mode	If setpoint are not calculated by NAZA Cores after 2s upon levers setpoints normal calculation (UC10-FNC-06), the supervisor shall enter back-up mode.	High
UC10-FNC-10	Levers setpoints sending normal mode	If supervisor is in normal mode upon Supervisor normal mode (UC10-FNC-08), the NAZA cores shall send topological orders, batteries setpoints and modulation orders calculated upon levers setpoints normal calculation (UC10-FNC-06) to corresponding NAZA acquisition every 5s.	High
UC10-FNC-11	Levers setpoints sending back-up mode	If supervisor is in back-up mode upon Supervisor back-up mode (UC10-FNC-09), the NAZA cores shall send topological orders, batteries setpoints and modulation orders calculated upon levers setpoints back-up calculation (UC10-FNC-07) to corresponding NAZA acquisition every 5s.	High

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-FNC-12	Supervisor fault mode	If no data is received from upper level after 10 minutes upon upper level acquisition (UC10-FNC-01, UC10-FNC-02, UC10-FNC-03), the supervisor shall enter fault mode.	High
UC10-FNC-13	Fault mode	If supervisor is in fault mode upon Supervisor fault mode (UC10-FNC-12), the NAZA cores shall send no levers setpoints information.	High
UC10-FNC-14	Supervisor mode change notification	If supervisor state changes, an alarm shall be displayed to the operator.	Medium
UC10-FNC-15	Trial mode	If supervisor is in trial mode upon operator demand, the NAZA cores shall send direct orders or setpoints to levers through HMI (mode used to check the new levers).	Medium
UC10-FNC-16	Event log	All events leading to an action of the system on the levers should be logged and accessible for 3 months.	Medium

Table 1 – UC10 Functional Requirements Description

4.1.2 Interface Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-INT-01	Upper level interface	The NAZA Cores shall use REST API to exchange with upper level	High
UC10-INT-02	SCADA Interface	The NAZA acquisition shall communicate with OPC-UA SCADA Gateway	High
UC10-INT-03	Hypervisor interface	The NAZA cores shall provide APIs to hypervisor system such as Operator Fabric to insert NAZA system in control room operator environment	High
UC10-INT-04	Interface sensors Interface	The NAZA acquisition shall communicate with IEC 61850 sensors	High
UC10-INT-05	Topological event Interface	The NAZA acquisition shall communicate with IEC 60870-5-104 Remote Transmission Units	High
UC10-INT-06	Topological orders Interface	The NAZA acquisition shall communicate with OPC-UA SCADA Gateway	High
UC10-INT-07	Batteries set points Interface	The NAZA acquisition shall communicate with Battery Management System with IEC 60870-5-104	High
UC10-INT-08	Generation Modulation Interface	The NAZA acquisition shall communicate with OPC-UA Generators and Distribution System Operators Gateways (*may evolve in next version)*	High
UC10-INT-09	Communications	All communications are on a private IP MPLS Wide Area Network. Bandwidth between NAZA Cores should be limited to 500 kb/s.	Medium
UC10-INT-10	Language	Java or C++ shall be used.	High

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-INT-11	Architecture	Implementation should be RESTful.	Medium

Table 2 – UC10 Interface Requirements Description

4.1.3 Performance Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-PRF-01	Availability	System shall be available at 99.99% of operation time	High
UC10-PRF-02	Dependability	No more than one unwanted order shall be sent every 10 years.	High
UC10-PRF-03	Algorithm duration	Algorithm (MPC based) shall provide results in less than 2s.	High
UC10-PRF-04	Orders transmission	An order elaborated by the algorithm must reach the adequate gateway in less than 5s, telecommunication delay excluded.	High
UC10-PRF-05	Invalid sensor measurement detection	Invalid measurement from sensors shall be detected in less than 10s	High
UC10-PRF-06	Alarm Manual mode change	A manual mode change (ie trial mode) should take less than 20 s.	Medium

Table 3 – UC10 Performance Requirements Description

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.1.4 Security Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-SEC-01	Operating system	Use of a secured Linux CentOS (7.4) is mandatory.	High
UC10-SEC-02	Identification	The use of RTE industrial Active Directory is mandatory.	High
UC10-SEC-03	Event log	A log shall trace all events linked to identification, access control, resources access and operation.	High

Table 4 – UC10 Security Requirements Description

4.1.5 Safety Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-SAF-01	Technical Order of 17/05/2001	Minimum distance between active conductors and ground or installation shall be guaranteed.	High
UC10-SAF-02	Safety of persons and goods	The system should never perform the reclosing of a circuit breaker without operator validation.	High
UC10-SAF-03	Physical component operating range	The physical operating ranges (power, load, …) of controlled components shall be respected and treated as constraints in algorithms.	High

Table 5 – UC10 Safety Requirements Description

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.1.6 Operational Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-OPR-01	Monitoring	Health of components, firmware or software version should retrieved automatically.	Medium
UC10-OPR-02	Advanced monitoring	The system may send an alert to upper level if in abnormal operation conditions and provide an advanced diagnosis based on individual logs.	Low
UC10-OPR-03	Remote provisioning	New sensors shall be configured remotely from central control room	High
UC10-OPR-04	Remote modelling modification	Control room operator should be able to remotely modify the modelling (configuration) data, for example in case of modification in the substation.	Medium
UC10-OPR-05	Remote code management	Control room operator should be able to install remotely a new version of the software on all concerned calculators.	Medium
UC10-OPR-06	Maintenance mode	When a substation or part of substation under the supervision of the area automata is in maintenance, data from these sensors shall be ignored or replaced by estimated data.	High
UC10-OPR-07	Advanced monitoring	The system should send an alert to upper level if in abnormal operation conditions and provide an advanced diagnosis based on individual logs.	Medium
UC10-OPR-08	Auto discovery	New sensors may be automatically detected by the application	Low
UC10-OPR-09	Dynamic resources allocation	Material resources (CPU, bandwidth, …) may be re-allocated dynamically to enhance performance or availability	Low

Table 6 – UC10 Operational Requirements Description

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.1.7 Usability Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-USB-01	Hypervisor compatibility	Information from the system shall be displayed the hypervisor system of the control room based on OperatorFabric.	High
UC10-USB-02	User mode	The interface should clearly separate the different users modes, such as operator mode, administration mode, logs.	Medium
UC10-USB-03	State of the system	The state of the system (on, off, out of order) shall always be visible in every screen of the interface.	High
UC10-USB-04	Graphic chart	The principles defined in the industrial IT graphic chart shall be respected (on=green, off=red, important alarm in red, low priority alarm in orange.	High
UC10-USB-05	Window organization	General rules for the window composition for control room operator shall apply: system state in upper left corner, user mode change in upper panel, view change in lateral left panel, alarms in upper part of main window.	Medium
UC10-USB-06	Internationalization	All Human Machine Interface should support different languages	Low

Table 7 – UC10 Usability Requirements Description

4.1.8 Policies & Compliance Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-P&C-01	French Military Programming Act	Specific security rules apply to operators of essential services.	High
UC10-P&C-02	European NIS Directive 2016/1148	The NIS Directive provides legal measures to boost the overall level of cybersecurity operators of essential services.	High
UC10-P&C-03	Open Source Software	Software developed by RTE should be Open Source if of interest for the Energy Community.	Medium

Table 8 – UC10 Policies & Compliance Requirements Description

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.1.9 Design Constraints

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-DSG-01	Hardware	Calculators and sensors gateway shall run on Intel powered servers.	High
UC10-DSG-02	Substation environment - Temperature	The operating range of the calculators shall be -10°C + 55°C. It could be restrained to 0°C -40°C if needed.	High

Table 9 – UC10 Design Constraints Requirements Description

4.1.10 Ethical Requirements

Requirement ID	Short Description	Description	Priority (H/M/L)
UC10-ETH-01	Data protection	No personal data shall be processed by the system. Commercially sensible data, such as load for consumers or production from generator shouldn't be store longer than required to achieve the system proper operation.	High
UC10-ETH-02	Liability	All system operation shall be explainable, ie curtailed generator should have, if asked, all information on why he was curtailed.	High
UC10-ETH-03	Global reliability	Global reliability of the system shall be assessed on a yearly basis to check if the requirements are reached and if not take corrective action.	Medium

Table 10 – UC10 Ethical Requirements Description

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2 UC 11 – Substation digitalization

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.1 The Titanium FMEA table

Equipment	Role	Failure modes	Effects		Détection	Comments
			Local	System		
Control server 11 (floating @ IP)	* monitors the status of compute servers 12 & 22 (heartbeat signal) * stores the context data enabling to transfer to control server 21 if needed * …	complete server crash (power supplies lost, UC failure, …)	loss of server 11	* compute servers 12 & 22 no more monitored by server 11 * server 21 automatically replaces server 11 * compute servers 12 & 22 managing ANSI protections are not affected	by server 21	* a control server failure cannot affect compute servers treatments * the server can be replaced in less than 3h (spare on site) * MTTR considered = 48h
		lost communication with one of the compute servers (e.g.server 12)	control server 11 communicates only with one of the compute servers (e.g. server 22)	* compute server 12 no more monitored by server 11 * server 21 replaced by server 11 * compute servers 12 & 22 not affected	by server 21	
		lost communication with control server 21	control server 11 only communicates with compute servers 12 & 22	* lost synchronisation between CTL servers * in case of server 11 loss, server 21 takes over without up to date context => possible malfunction of automation functions, but no impact on distance and overcurrent protections	by server 21	
		failure of remote maintenance port OAM	no effect	increased MTTR in case of failure	loss of communication	* this port enables a remote intervention in case of trouble * typical MTTF for a switch ~1E6h
Compute server 12	* receives in IEC 61850 protocole the analogue mesurements (U,I) and the status information (DI) sent by field equipment (MU + SMTB) * supports virtual machines ensuring ANSI protection functions * remotely controls via IEC 61850 links the switchgear manoeuvers (tripping on fault, opening/closing) * …	server crash (power supplies, UC failure, …)	loss of server 12 => automation & protection functions no more performed by this server	* server 22 not impacted, goes on ensuring these functions * failure detected by the control servers => alarm and server 12 replacement	active control server 11	* no impactthanks to compute server 22 redundancy * the server can be replaced in less than 3h (spare on site) * MTTR considered = 48h
		lost communication with active control server (e.g. server 11)	compute server 12 no more monitored by active control server 11, but still monitored by standby control server 21	* automatic switch from server 11 to server 21 * compute servers 12 & 22 not impacted	control server 11	
		lost communication with standby control server (e.g. server 21)	compute server 12 remains monitored by active control server 11, but no more by standby control server 22	* no effect on single fault * lost communication is detected by server 21 => alarm & replacement of faulty server 12 (or faulty communication card)	control server 21	
		lost communication with a switch (e.g. network A)	compute server 12 cannot communicate with the field on network A	* communication still valid through IEC 61508 network B => no impact at first fault * lost communication detected by server 12 => alarm, diagnostic, repair	server 12	PRP switch considered
		lostcommunication with compute server 22	compute server 12 cannot communicate with redundant compute server 22	* server 12 functions not impacted => no effect on single fault * lost communication detected by the server => alarm, diagnostic, repair	server 12	
		spurious tripping command to the circuit breaker	switch A receives an undue tripping command	spurious tripping of circuit breaker	no	* very unlikely (IEC 61850 protocole with CRC, etc) * STB_DO module does not check the consistency between switch A vs switch B messages * breaker tripping detected by breaker feedback signal
		lost tripping command to circuit breaker	VM error or HW failure preventing from sending a breaker tripping command	compute server 12 can still send commands through independent switch B, having its own medium (different commands on redundant networks)	no	very unlikely
		communication freezing communication networks A by deny of service	frozen communication network A	no impact on single fault : communication network B remains OK and enables to operate the system	lost of communication network A	very unlikely ; the virtual networks segregation (VLAN) reduces the risks of total network breakdown, with maximum allowable bandwidths for each VLAN.
Ultrafast infrastructure switch	used for VMs migration and backup actuation between compute servers	infrastructure port failure management + infra	lost infrastructure port	loss of VMs migration functions => above listed backups lost	lost of communication	ANSI functions can be affected by dual failure scenario
Grand Master Clock	used for servers synchronisation => critical for certain protectionfunctiond, if different SAMU are used	failure of GPS or lost communication with both switches	lost synchro	lost SOE consistancy.Protections using different Mus are lost	lost communication switches A & B	synchronises the MUs => causes the loss of differential & synchrocheck protections, but no impact on distant and overcurrent protections if a single MU is used

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.2 ANSI 50/51 & 21 - Fault tree analysis

Based on the analyses performed in the previous steps, a complete model can be elaborated for the SDEC solution, and for the Easergy relay as well.

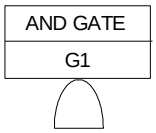
The models are based on the fault tree methodology, which enable:

- To take multiple failure scenarios into consideration (where FMEAs only address individual failures, one by one)
- An easy understanding of the combinations of failures leading to each critical event studied (eases the verification).

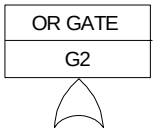
The FTA models are detailed in the following sections.

In order to keep this dependability report simple, only the fault trees related to the distant protection ANSI 21 are given. Those concerning the overcurrent protection function ANSI 50/51 are both simpler, and less critical.

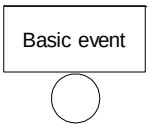
Fault Tree Analysis symbols



This symbol represents an AND GATE. The output of this gate is true if all input events are true simultaneously. If all inputs are independents, then $P_{Gate} \approx \prod_i Pi$



This symbol represents an OR GATE. The output of this gate is TRUE if at least one input event is true. $P_{Gate} \approx \sum_i Pi$



This symbol represents a BASIC EVENT that is the failure of a component with which a statistic law is associated. $P(t) = 1 - R(t) = 1 - e^{-\lambda t}$

List of basic events used in the FTA

Basic event	Definition
com12 A	failure of the communication port A of the server 12
com12 B	failure of the communication port B of the server 12
com22 A	failure of the communication port A of the server 22
com22 B	failure of the communication port B of the server 22
COM61850_DD	detected failure of the STB IEC 61850 communication module
comCPS12->11	loss of communication between servers 11 and 12
comCPS12->22	loss of communication between servers 12 and 22
COMTB_DD	dangerous detected failure of the STB communication module (protection masking)
COMTB_S	safe failure of the STB communication module (spurious trip)
CPS12_DD	dangerous detected failure of the compute server 12 (protection masking)
CPS12_DU	dangerous undetected failure of the compute server 12 (protection masking)
CPS12_SU	safe undetected failure of the compute server 12 (spurious trip)
CPS22_DD	dangerous detected failure of the compute server 22 (protection masking)
CPS22_DU	dangerous undetected failure of the compute server 22 (protection masking)
CPU30_21_DD	dangerous detected failure of Easergy CPU board (ANSI 21 masking)
CPU30_21_DU	dangerous undetected failure of Easergy CPU board (ANSI 21 masking)
CPU30_21_S	safe failure of Easergy CPU board (spurious trip ANSI 21)
crash-CTLS11	complete loss of control server 11
crash-CTLS21	complete loss of control server 21
CTbox1_21_DD	dangerous detected failure of the CT card channel 1 (ANSI 21 masking)
CTbox1_21_S	safe failure of the CT card channel 1 (ANSI 21 tripping)
CTbox2_21_DD	dangerous detected failure of the CT card channel 2 (ANSI 21 masking)
CTbox2_21_S	safe failure of the CT card channel 2 (ANSI 21 tripping)
CTbox3_21_DD	dangerous detected failure of the CT card channel 3 (ANSI 21 masking)
CTbox3_21_S	safe failure of the CT card channel 3 (ANSI 21 tripping)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

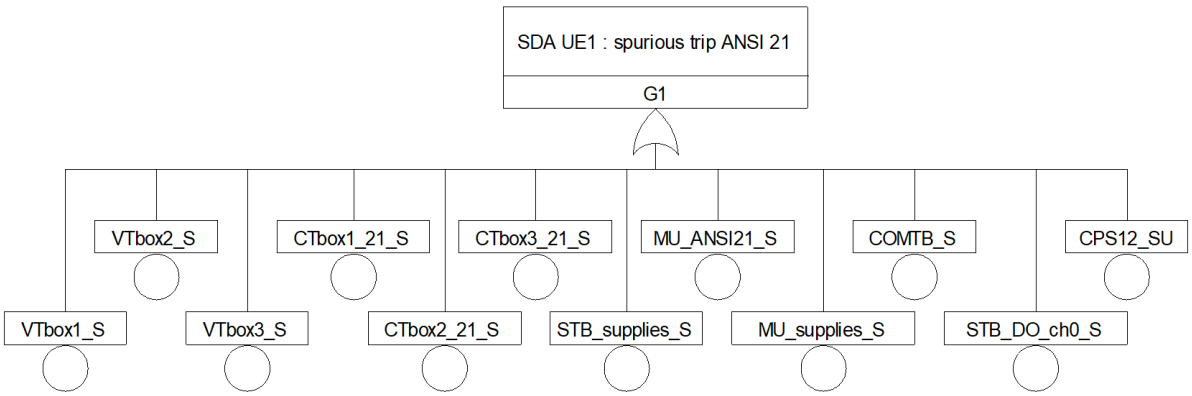
Basic event	Definition
DenSce12 A	failure of the communication port A of the server 12
DenSce12 B	failure of the communication port B of the server 12
DenSce22 A	failure of the communication port A of the server 22
DenSce22B	failure of the communication port B of the server 22
MU_ANSI21_DD	detected failure of the STB IEC 61850 communication module
MU_ANSI21_S	loss of communication between servers 11 and 12
MU_SFP1	loss of communication between servers 12 and 22
MU_SFP2	dangerous detected failure of the STB communication module (protection masking)
MU_supplies_DD	safe failure of the STB communication module (spurious trip)
MU_supplies_S	dangerous detected failure of the compute server 12 (protection masking)
PSU30H_DD	dangerous detected failure of Easergy power supplies (ANSI 21 masking)
PSU30H_DU	dangerous undetected failure of Easergy power supplies (ANSI 21 masking)
PSU30H_S	safe failure of Easergy power supplies (spurious trip ANSI 21)
STB_DO_ch0_DD	dangerous detected failure of STB DO channel 0 (ANSI 21 masking)
STB_DO_ch0_DU	dangerous undetected failure of STB DO channel 0 (ANSI 21 masking)
STB_DO_ch0_S	safe failure of STB DO channel 0 (spurious trip ANSI 21)
STB_supplies_DD	dangerous detected failure of STB power supplies (ANSI 21 masking)
STB_supplies_DU	dangerous undetected failure of STB power supplies (ANSI 21 masking)
STB_supplies_S	safe failure of STB power supplies (spurious trip ANSI 21)
switch A	loss of communication switch A
switch B	loss of communication switch B
switch-infrastr	loss of Titanium infrastructure switch
VTbox1_21_S	dangerous detected failure of the VT card channel 1 (ANSI 21 masking)
VTbox1_S	safe failure of the VT card channel 1 (ANSI 21 tripping)
VTbox2_21_S	dangerous detected failure of the VT card channel 2 (ANSI 21 masking)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

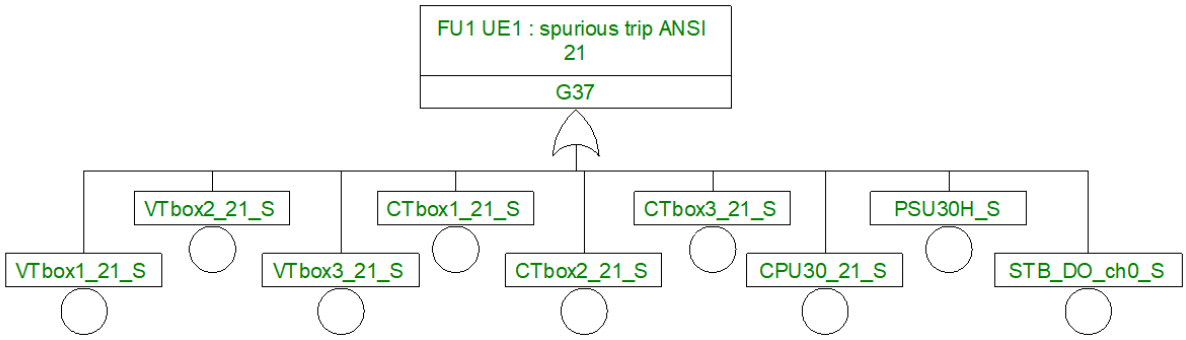
Basic event	Definition
VTbox2_S	safe failure of the VT card channel 2 (ANSI 21 tripping)
VTbox3_21_S	dangerous detected failure of the VT card channel 3 (ANSI 21 masking)
VTbox3_S	safe failure of the VT card channel 3 (ANSI 21 tripping)

FTA – UE1 (spurious trip of ANSI 21 – scenario 1)

SDEC solution



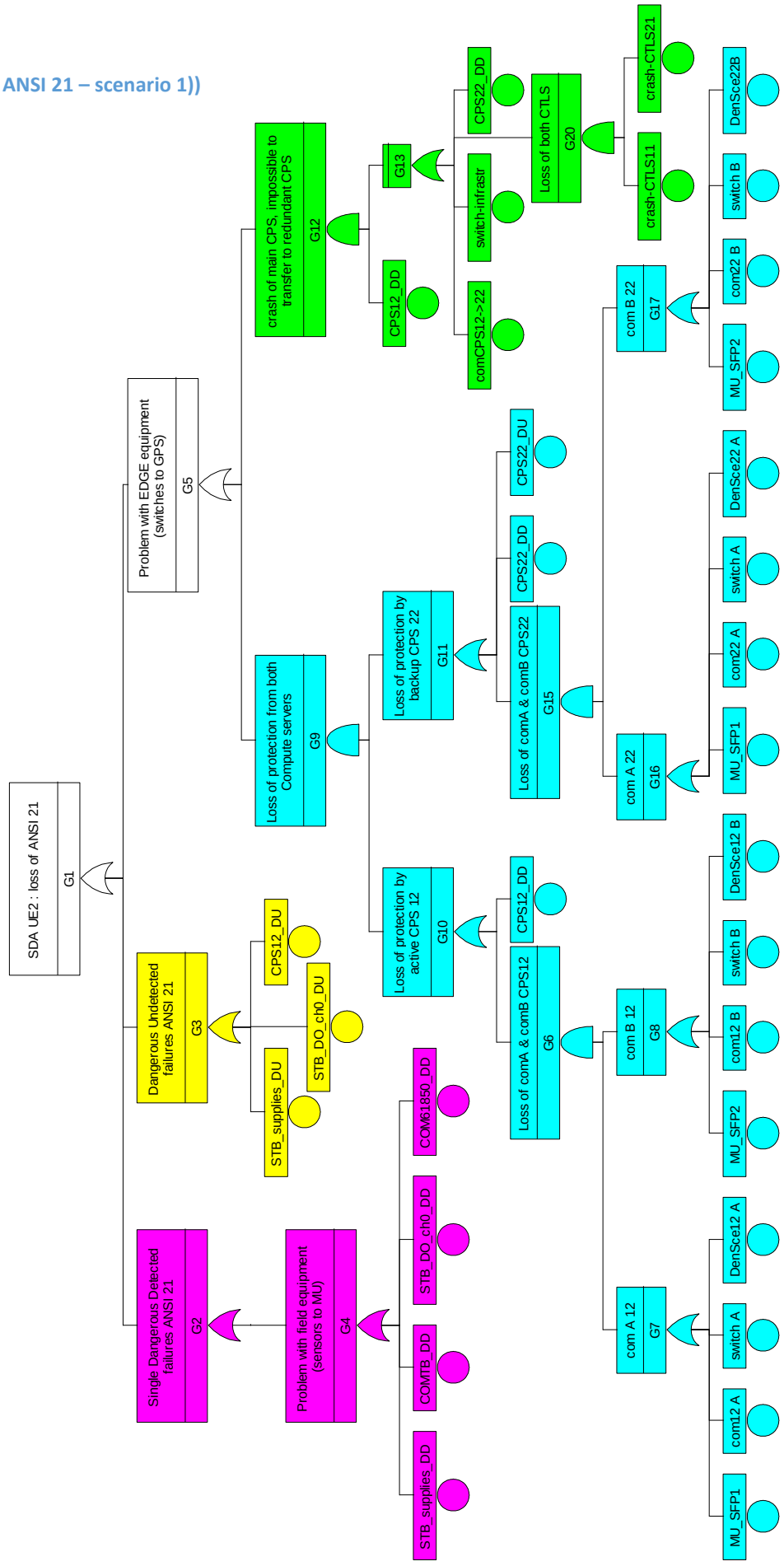
Easergy IED



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

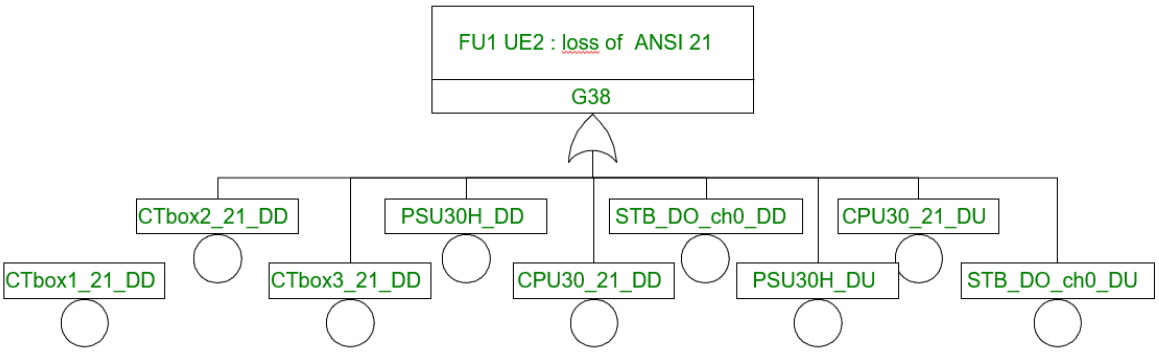
UE1 FTA - UE2 (loss of ANSI 21 – scenario 1))

SDEC solution



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Easergy IED

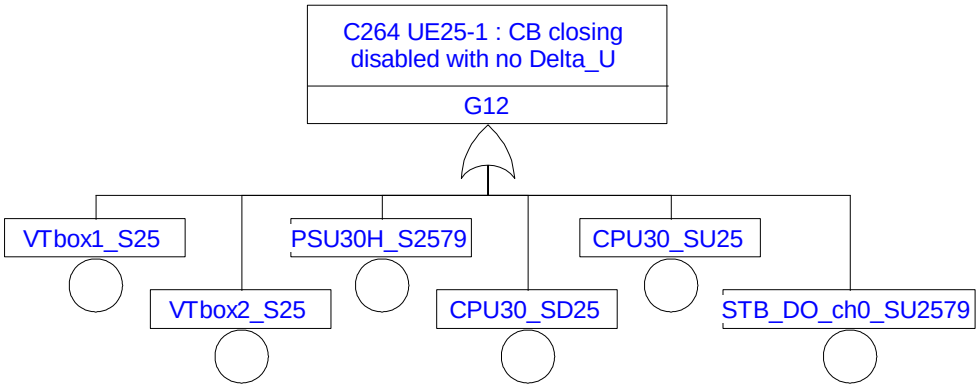


This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.3 ANSI 25 - fault tree analysis

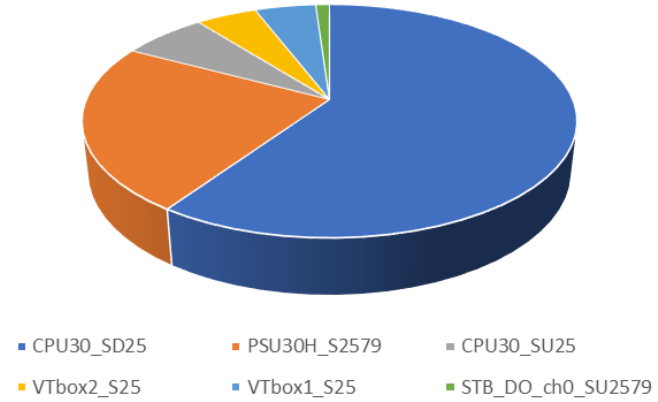
FTA – UE25-1 (spurious actuation of the ANSI 25 function)

C264-like solution



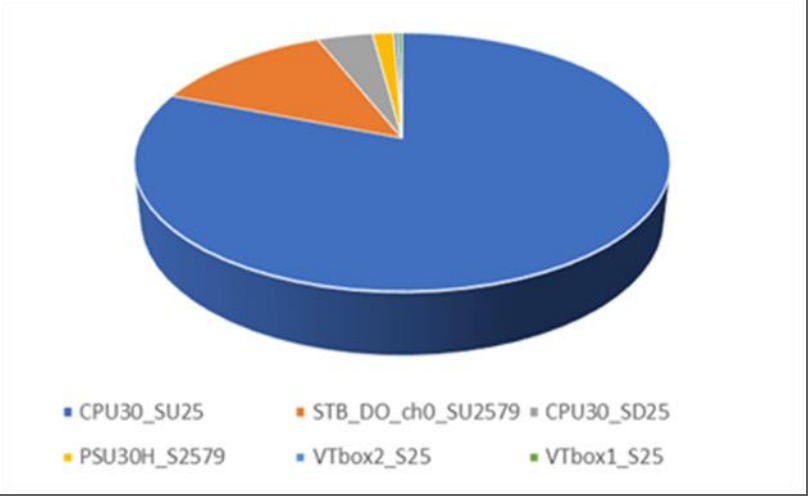
This FTA leads to the results below:

Equivalent failure rate for UE25-1 λ_{UE25-1} /h	Main contributors to λ_{UE25-1}	
1,13E-06	CPU30_SD25	59,5%
	PSU30H_S2579	23,2%
	CPU30_SU25	6,6%
	VTbox2_S25	4,8%
	VTbox1_S25	4,8%
	STB_DO_ch0_SU25	1,1%

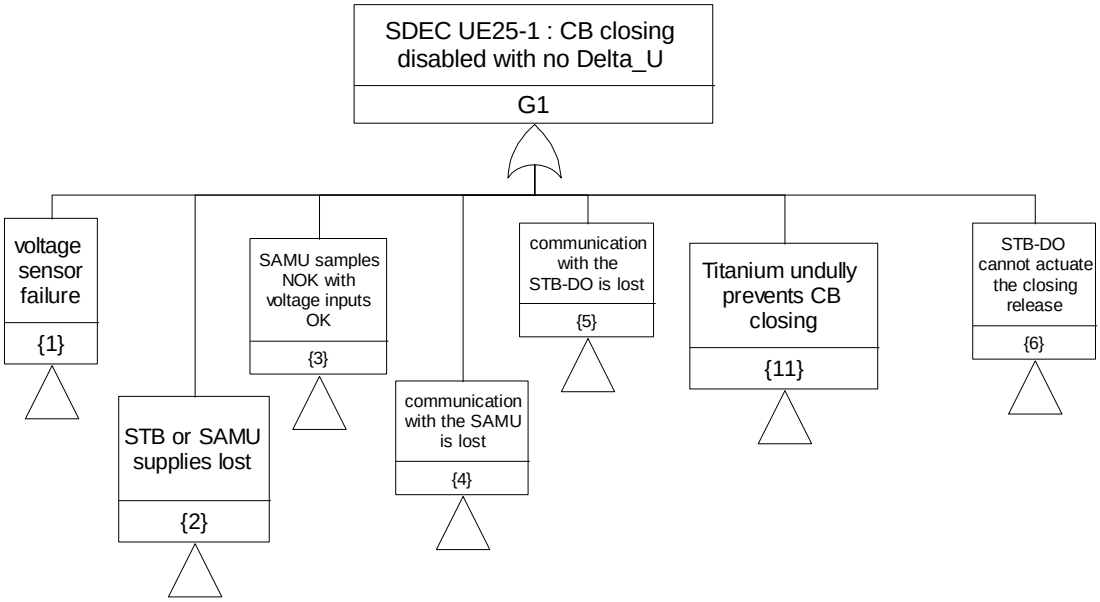


This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

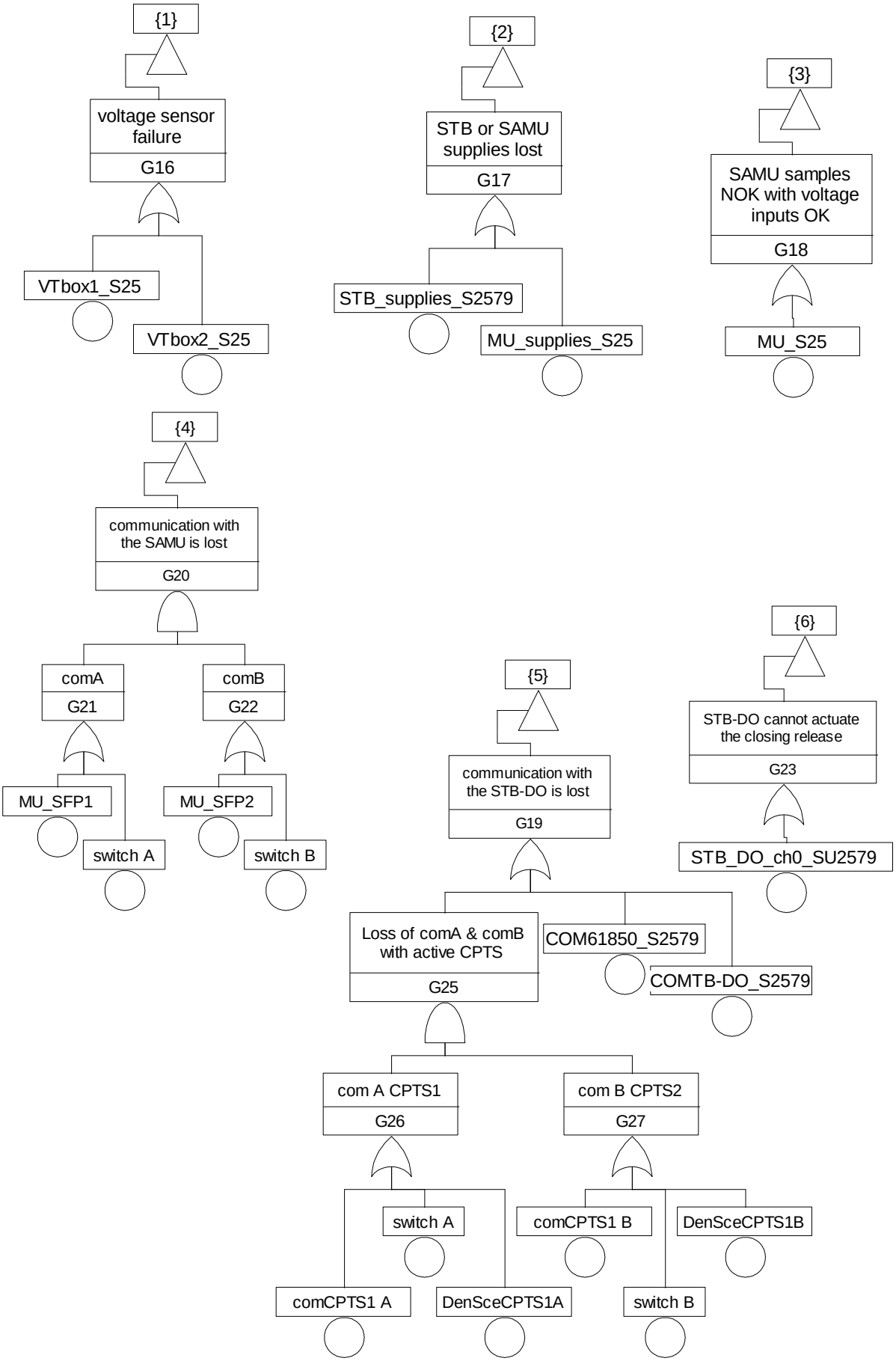
Mean probability of UE25-1 P UE25-1	Main contributors to P UE25-1
4,35E-04	CPU30_SU25 80,9% STB_DO_ch0_SU2579 13,0% CPU30_SD25 4,0% PSU30H_S2579 1,5% VTbox2_S25 0,3% VTbox1_S25 0,3%



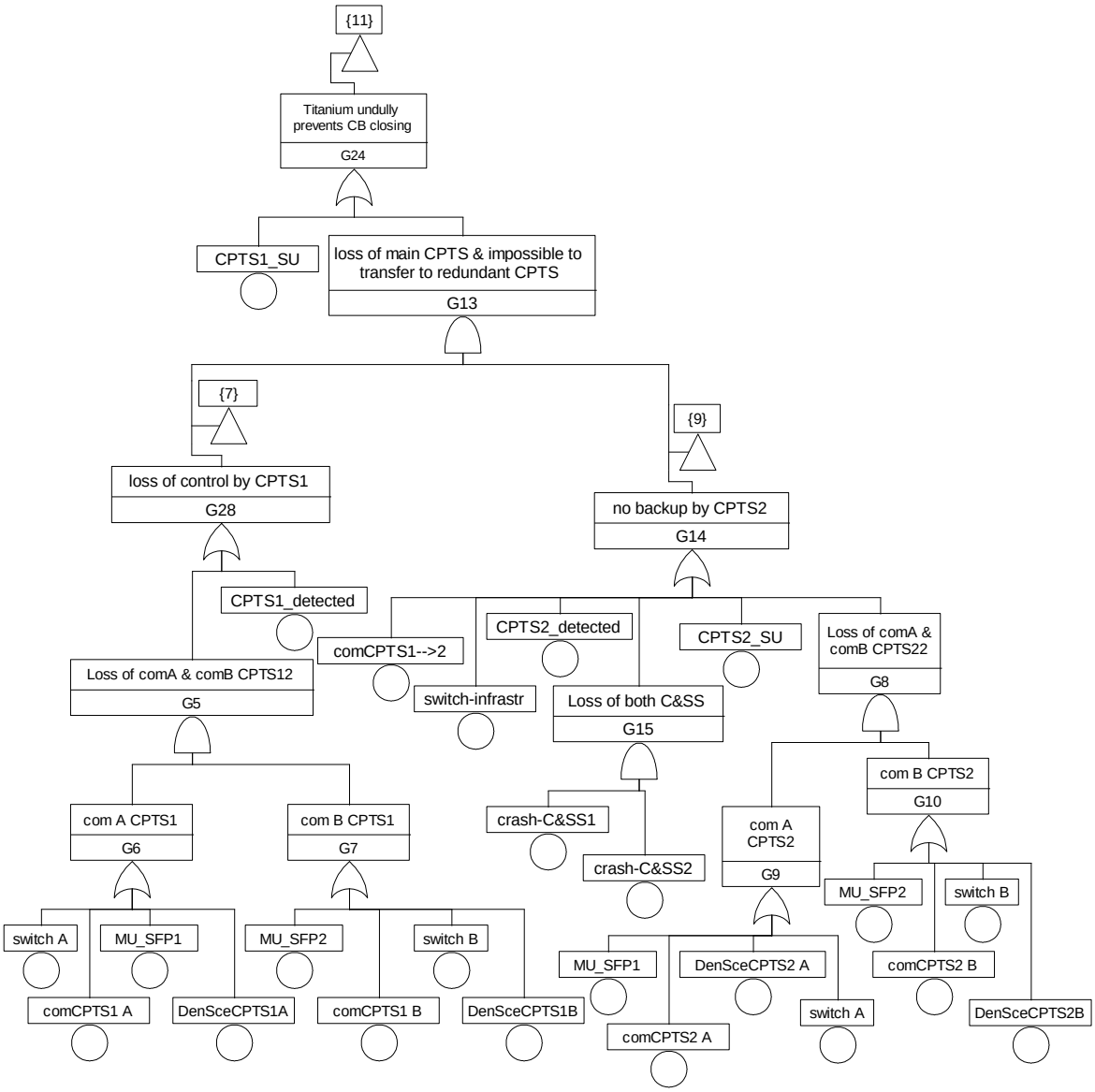
SDEC solution



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276



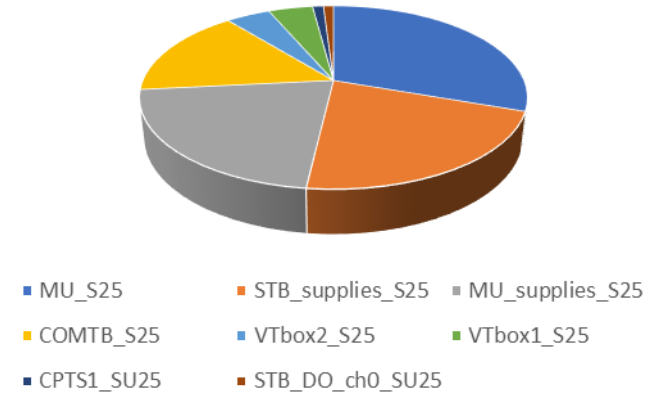
This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

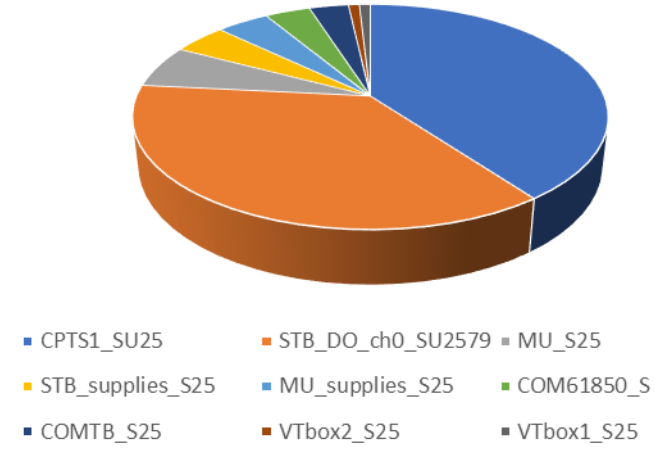


Resulting in:

Mean probability of UE25-1 **P UE25-1**	**Main contributors to P UE25-1**	
1,22E-06	MU_S25	30,3%
	STB_supplies_S25	21,5%
	MU_supplies_S25	21,5%
	COMTB_S25	15,7%
	VTbox2_S25	4,4%
	VTbox1_S25	4,4%
	CPTS1_SU25	1,1%
	STB_DO_ch0_SU25	1,0%

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

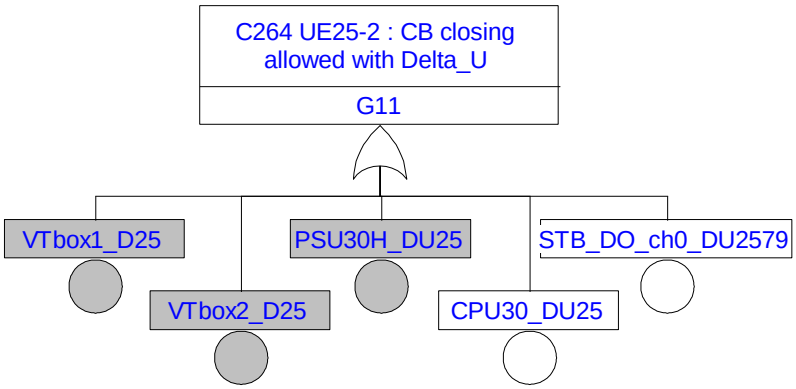
Mean probability of UE25-1 P_{UE25-1}	Main contributors to P_{UE25-1}
1,22E-06	

Mean probability of UE25-1 P_{UE25-1}	Main contributors to P_{UE25-1}
1,78E-04	CPTS1_SU25 39,8% STB_DO_ch0_SU2579 36,7% MU_S25 6,1% STB_supplies_S25 4,4% MU_supplies_S25 4,3% COM61850_S 3,7% COMTB_S25 3,2% VTbox2_S25 0,9% VTbox1_S25 0,9% 

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

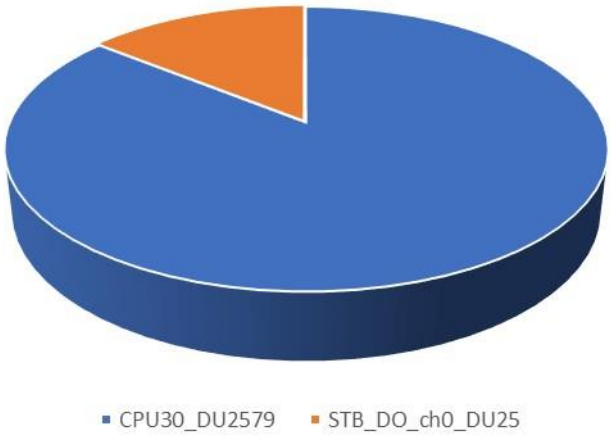
FTA – UE25-2 (loss of the ANSI 25 function)

C264-like solution

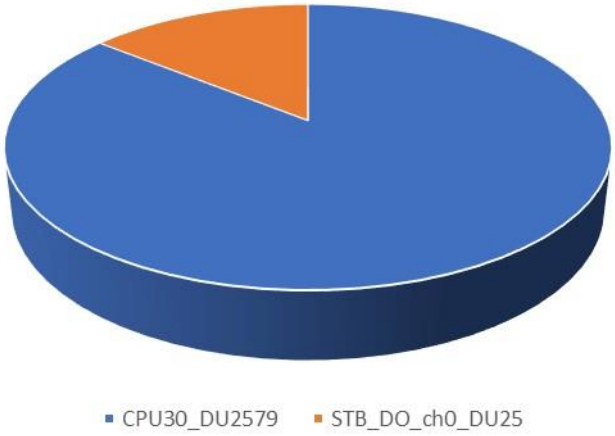


Note : on this fault tree, events shown in grey boxes are single failures that shall theoretically be considered, but that in fact cannot occur (the associated failure rate is zero).

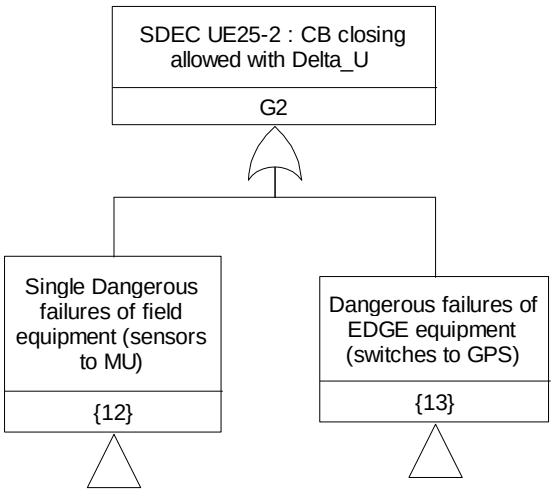
After FTA resolution, the results are:

Mean probability of UE25-2 P_{UE25-2}	Main contributors to P_{UE25-2}
3,43E-08	CPU30_DU25 85,80% STB_DO_ch0_DU2579 14,20% 

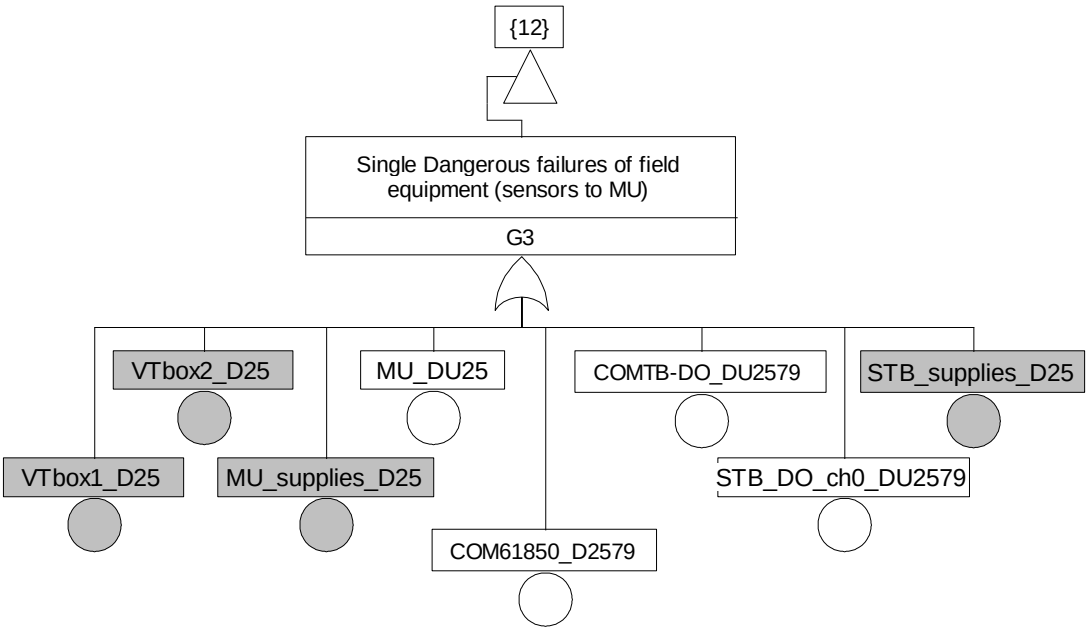
This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Mean probability of UE25-2 P UE25-2	Main contributors to P $_{UE25-2}$
1,50E-04	CPU30_DU25 85,80% STB_DO_ch0_DU2579 14,20% 

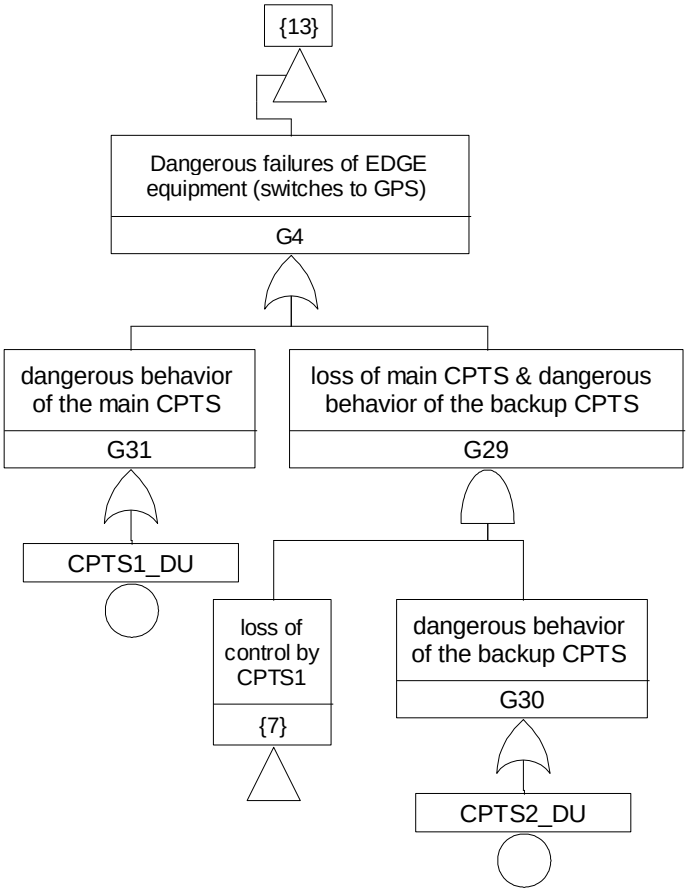
SDEC solution



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

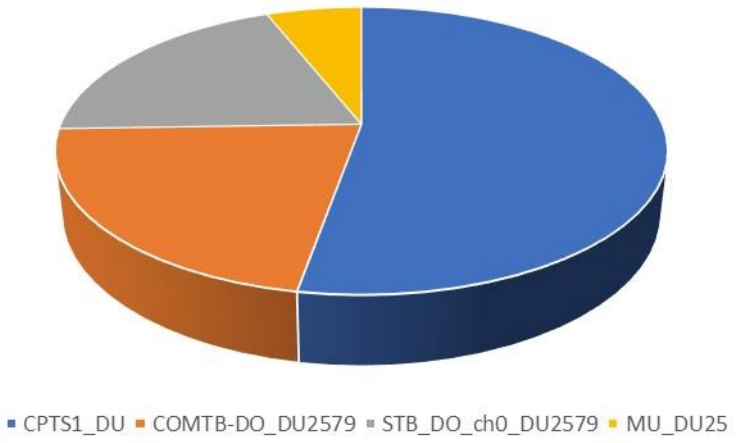


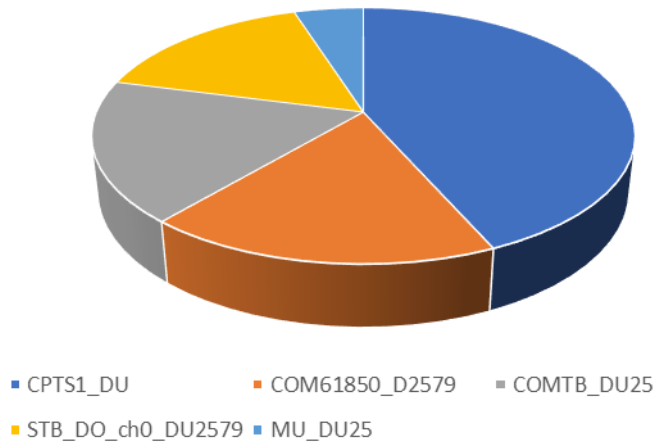
Note : on this fault tree, basic events shown in grey boxes have a failure rate equal to zero.



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Which implies the following results:

Equivalent failure rate for UE25-2 λ_{UE25-2} /h	Main contributors to P_{UE25-2}
2,50E-08	CPTS1_DU 52,80% COMTB-DO_DU2579 21,70% STB_DO_ch0_DU2579 19,50% MU_DU25 6,00% 

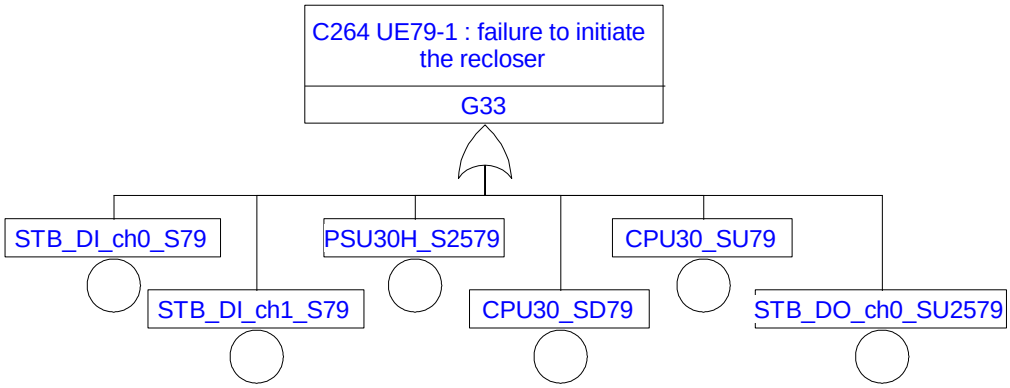
Mean probability of UE25-2 P_{UE25-2}	Main contributors to P_{UE25-2}
1,33E-04	CPTS1_DU 43,4% COM61850_D2579 17,8% COMTB_DU25 17,8% STB_DO_ch0_DU2579 16,0% MU_DU25 4,9% 

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.4 ANSI 79 - fault tree analysis

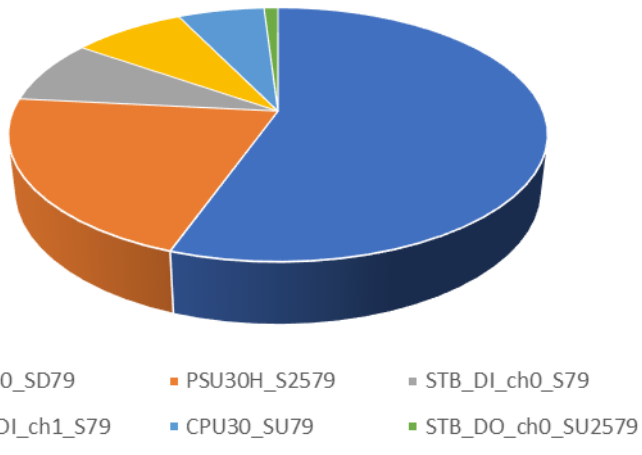
FTA – UE79-1 (failing to re-close the breaker automatically)

C264-like solution



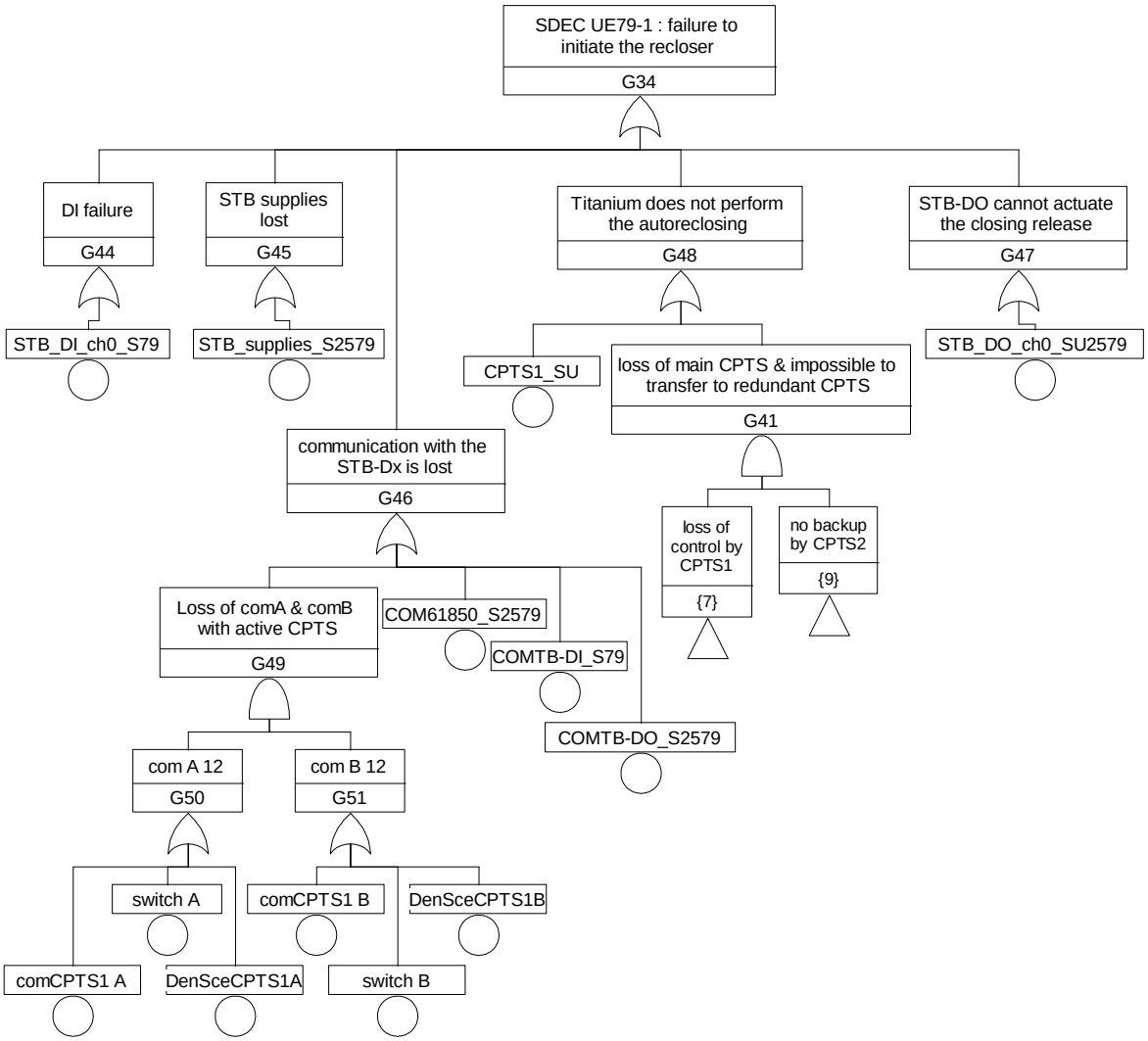
This FTA leads to the results below:

Equivalent failure rate for UE79-1 λ_{UE79-1} /h	Main contributors to P $_{UE79-1}$
1,22E-06	CPU30_SD79 55,50% PSU30H_S2579 21,20% STB_DI_ch0_S79 8,10% STB_DI_ch1_S79 8,10% CPU30_SU79 6,20% STB_DO_ch0_SU2579 1,00%



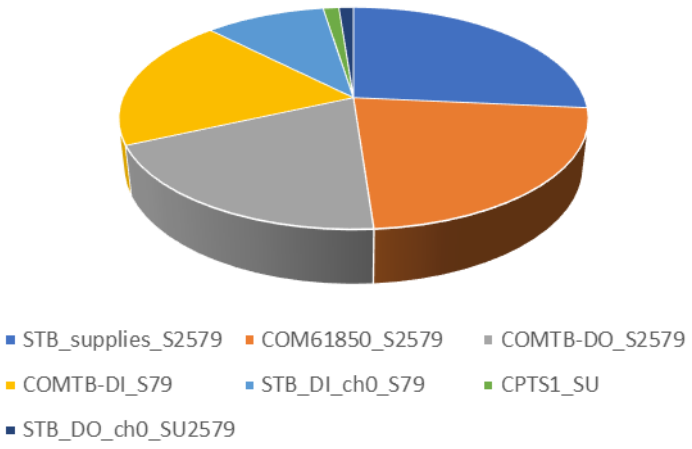
This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

SDEC solution

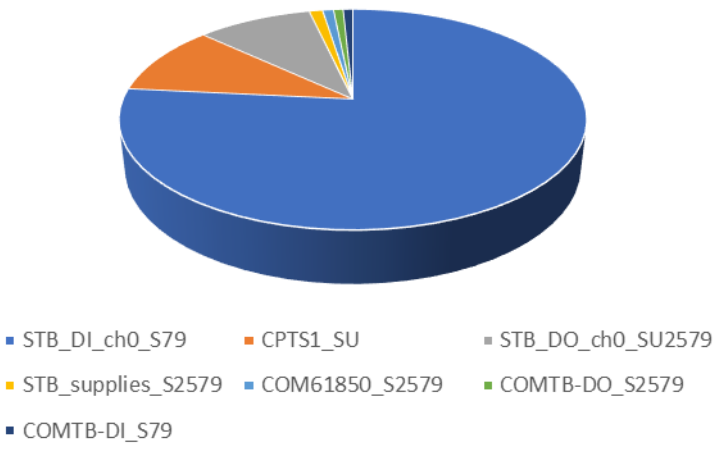


Resulting in:

Equivalent failure rate for UE79-1 λ_{UE79-1} /h	Main contributors to P_{UE79-1}	
9,94E-07	STB_supplies_S2579	26,50%
	COM61850_S2579	22,40%
	COMTB-DO_S2579	19,40%
	COMTB-DI_S79	19,40%
	STB_DI_ch0_S79	9,90%
	CPTS1_SU	1,30%
	STB_DO_ch0_SU2579	1,20%



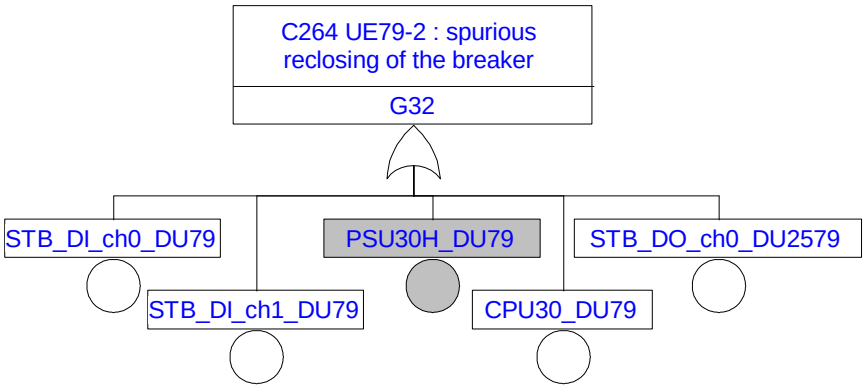
Mean probability of UE79-1 P_{UE79-2}	Main contributors to P_{UE79-2}	
5,82E-04	STB_DI_ch0_S79	76,50%
	CPTS1_SU	10,30%
	STB_DO_ch0_SU2579	9,50%
	STB_supplies_S2579	1,10%
	COM61850_S2579	0,90%
	COMTB-DO_S2579	0,80%
	COMTB-DI_S79	0,80%



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

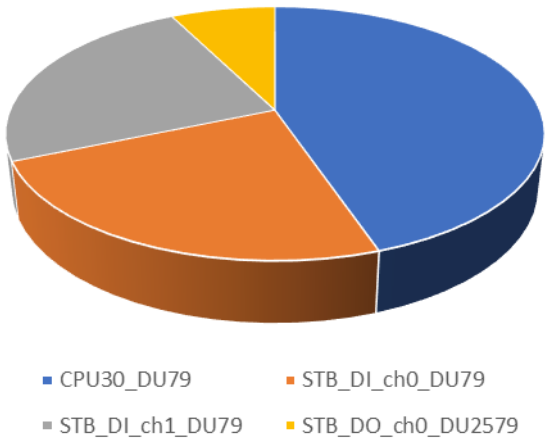
FTA – UE25-2 (spurious reclosing of the breaker)

C264-like solution

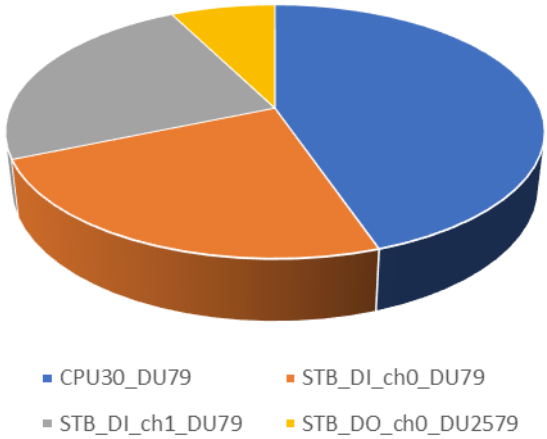


Note : on this fault tree, basic events shown in grey boxes have a failure rate equal to zero.

After FTA resolution, the results are:

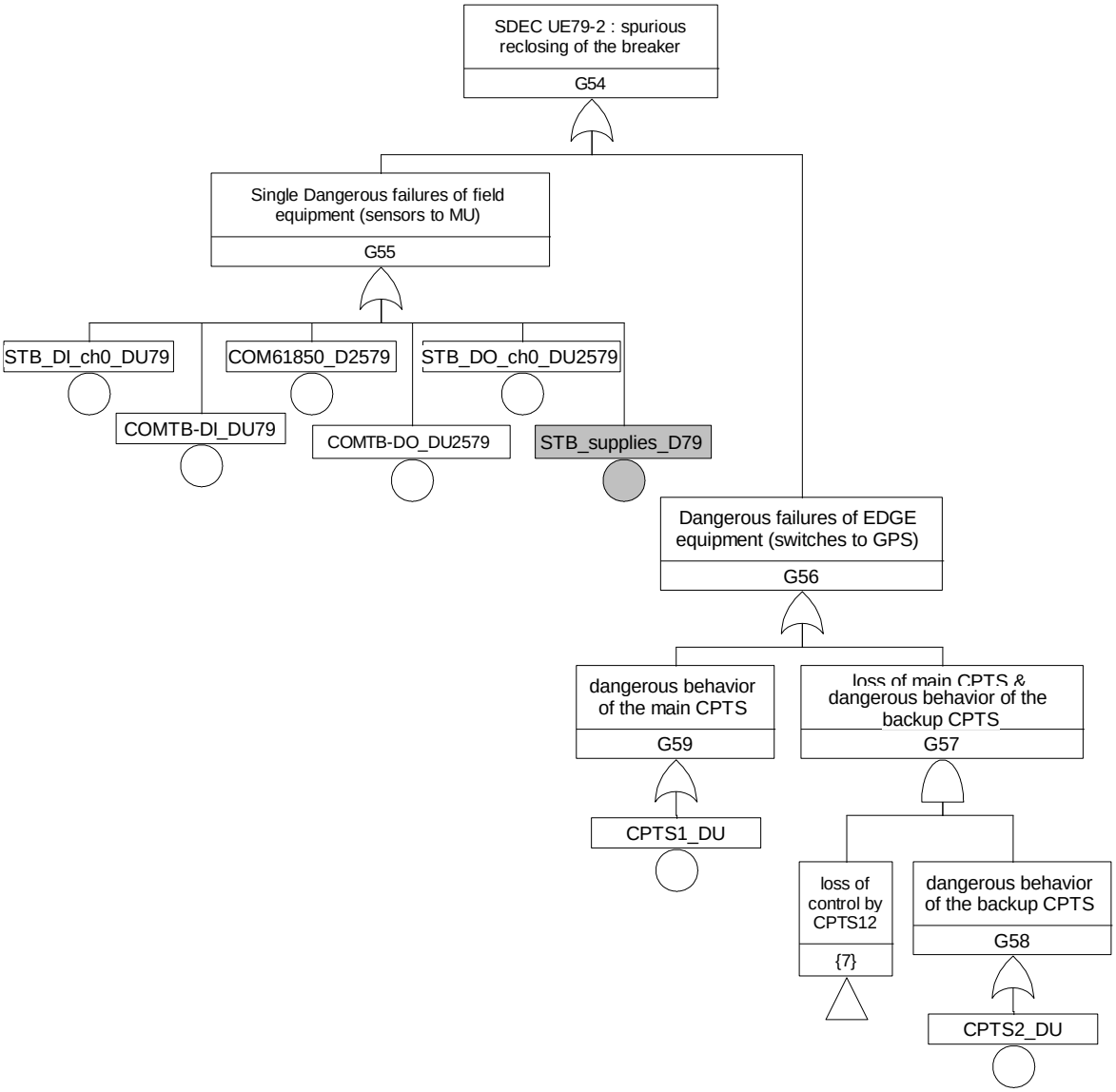
Equivalent failure rate for UE79-2 λ_{UE79-2} /h	Main contributors to P_{UE79-2}
6,48E-08	CPU30_DU79 44,80% STB_DI_ch0_DU79 23,90% STB_DI_ch1_DU79 23,90% STB_DO_ch0_DU2579 7,50% 

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Mean probability of UE79-2 P_{UE79-2}	Main contributors to P_{UE79-2}
2,84E-04	CPU30_DU79 44,80% STB_DI_ch0_DU79 23,90% STB_DI_ch1_DU79 23,90% STB_DO_ch0_DU2579 7,50% 

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

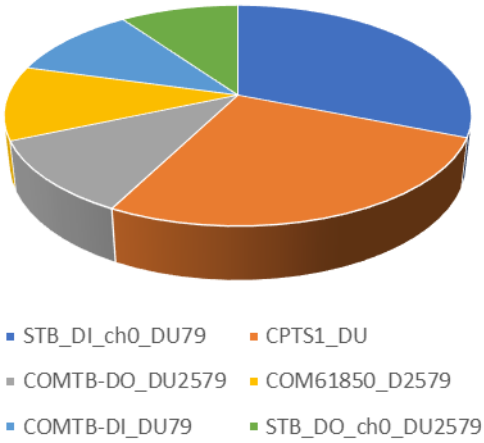
SDEC solution

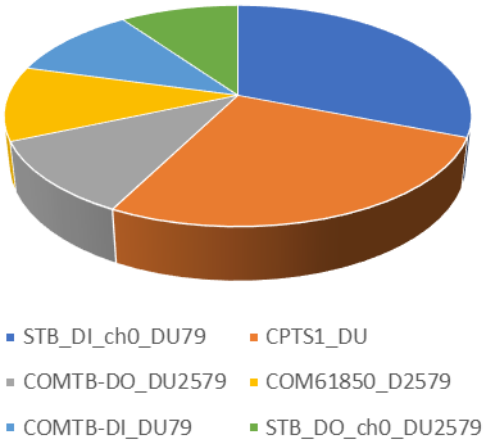


Note : on this fault tree, basic events shown in grey boxes have a failure rate equal to zero.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Which implies the following results:

Equivalent failure rate for UE79-2 λ_{UE79-2} /h	Main contributors to λ_{UE79-2}
5,00E-08	STB_DI_ch0_DU79 31,1% CPTS1_DU 26,5% COMTB-DO_DU2579 10,9% COM61850_D2579 10,9% COMTB-DI_DU79 10,9% STB_DO_ch0_DU2579 9,8% 

Mean probability of UE79-2 P_{UE79-2}	Main contributors to λ_{UE79-2}
2,18E-04	STB_DI_ch0_DU79 31,0% CPTS1_DU 26,5% COMTB-DO_DU2579 10,9% COM61850_D2579 10,9% COMTB-DI_DU79 10,9% STB_DO_ch0_DU2579 9,8% 

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.5 Electronics FMEA tables template

			Qualitative part			Quantitative part				POC RTE 2018 (shunt tripping coil)				
Function name	Sub function name	Component identification	Failure mode	Local Effect	$\lambda_{component}$	Repartition of the failure mode	Number of components	λ_{mode}	Unwanted events seen by the customer	Detection (0->1 trip)	loss of ANSI50	spurious ANSI50/51 actuatio	loss of ANSI2	spurious ANSI21 actuatio
FPGA	1V2 decoupling	C109, C112, C115, C118, C121, C124, C127, C128	S.C	Loss of the 1V2 power supply	5,68E-10	90%	8	4,0915E-09	UE2 : failure to trip	Reset	DD		DD	
FPGA	1V2 decoupling	C109, C112, C115, C118, C121, C124, C127, C128	O.C	Without effects	5,68E-10	10%	8	4,5461E-10	UE21: Without effect	NO				
FPGA	3V3 decoupling	C116, C117, C119, C120, C122, C123, C125, C126, C175	S.C	Loss of the 3V3 power supply	5,68E-10	90%	12	6,1372E-09	UE2 : failure to trip	Reset	DD		DD	
FPGA	3V3 decoupling	C116, C117, C119, C120, C122, C123, C125, C126, C175	O.C	Without effects	5,68E-10	10%	12	6,8191E-10	UE21: Without effect	NO				
FPGA	VCCA decoupling	C129, C131, C133	S.C	Loss of the 2V5 power supply	5,68E-10	90%	3	1,5343E-09	UE2 : failure to trip	Reset	DD		DD	
FPGA	VCCA decoupling	C129, C131, C133	O.C	Without effects	5,68E-10	10%	3	1,7048E-10	UE21: Without effect	NO				
FPGA	VCCA filtering	L11	S.C	Without effects	1,34E-09	20%	1	2,6771E-10	UE21: Without effect	NO				
FPGA	VCCA filtering	L11	O.C	Loss of the analog FPGA power supply	1,34E-09	80%	1	1,0708E-09	UE2 : failure to trip	Detected by CPU	DD		DD	
FPGA	VCCD_PLL decoupling	C130, C132, C134	S.C	Loss of the 1V2 power supply	5,68E-10	90%	3	1,5343E-09	UE2 : failure to trip	Reset	DD		DD	
FPGA	VCCD_PLL decoupling	C130, C132, C134	O.C	Without effects	5,68E-10	10%	3	1,7048E-10	UE21: Without effect	NO				
FPGA	VCCD_PLL filtering	L12	S.C	Without effects	1,34E-09	20%	1	2,6771E-10	UE21: Without effect	NO				
FPGA	VCCD_PLL filtering	L12	O.C	Loss of the PLL FPGA power supply	1,34E-09	80%	1	1,0708E-09	UE2 : failure to trip	Detected by CPU	DD		DD	
FPGA	nSTATUS PU	R75	O.C	Without effects	4,70E-11	100%	1	4,7047E-11	UE21: Without effect	NO				
FPGA	CONF_DONE PU	R76	O.C	Without effects	4,70E-11	100%	1	4,7047E-11	UE21: Without effect	NO				
FPGA	led debug	R77	O.C	Without effects	4,70E-11	100%	1	4,7047E-11	UE21: Without effect	NO				
FPGA	FPGA	U2	Safe		1,09E-07	0%	1	0	UE1: Spurious trip	NO		S		S
FPGA	FPGA	U2	Dangerous		1,09E-07	100%	1	1,0864E-07	UE2: Failure to trip	CRC, ...	DD		DD	
FPGA	HRESETn	C283	S.C	Reset	1,89E-10	70%	1	1,3259E-10	UE2: Failure to trip	Reset	DD		DD	
FPGA	HRESETn	C283	O.C or drift	Without effects	1,89E-10	30%	1	5,6826E-11	UE21: Without effect	NO				
FPGA	FPGA	R277, R278, R279, R280	O.C	Without effects	4,70E-11	100%	1	4,7047E-11	UE21: Without effect	NO				

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2.6 Reference documents

Ref	Doc .Number	Title	Date / Rev	Source
[1]	NHA8953920	STB DI electronics scheme	rev02	Schneider Electric
[2]	NHA8954118	STB DO electronics scheme	rev00	Schneider Electric
[3]	QGH4421323	CEI61850 converter electronics scheme	rev01	Schneider Electric
[4]	NVE1285201	CEI61850 converter power supplies electronics scheme	rev02	Schneider Electric
[5]	NHA8954220	COM_TB module (STB controls) electronics scheme	rev03	Schneider Electric
[6]	MU_SB SCH	CT/VT module electronics scheme	rev01 sept.2015	Schneider Electric
[7]	DFMEA_FUSION_IED_V1	Easergy Fusion v1 protection relay detailed FMEA	A11	Schneider Electric
[8]	WRTSRAM	Titanium Server RAM Modelling Analysis	4.0 Jan. 2015	KerrNet Consulting Inc.
[9]	IEC 62380	Reliability data handbook for reliability prediction of electronics components, PCBs and equipment	August 2004	IEC
[10]	IMdR – GTR 63	« Démarche et méthodes de Sûreté de Fonctionnement des logiciels »	Ed.2 April 2013	**I**nstitut pour la **M**aîtrise **d**es **R**isques

End of document

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276